MATH 215A Notes

Jiantong Liu

January 19, 2023

Preliminaries

This document is the notes based on Dr. Chengxi Wang's teaching at UCLA's 215A in fall 2022. The recommended textbook is Atuyah-MacDonald's *Introduction to Commutative Algebra* and David Eisenbud's *Commutative Algebra: with a View Toward Algebraic Geometry*.

1 Rings and Ideals

The study of commutative algebra started from commutative rings. We start from here and review a list of concepts that were built upon that.

Definition 1.1 ((Commutative) Ring)**.** A ring A is a set with two binary operations, usually called addition and multiplication, such that

- A is an Abelian group with respect to addition.
- The multiplication is associative and distributive over addition. (That is, A is a monoid with respect to multiplication.

We only think of rings that are commutative, that is, $xy = yx$ for all $x, y \in A$.

In this whole chapter, we think of rings to be commutative and with a multiplicative identity 1.

Remark 1.2. We say R is a trivial ring if and only if $1 = 0$, if and only if $R = 0$.

Example 1.3. Some examples include basic number rings like $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, polynomial rings $R[x_1, \cdots, x_n]$ constructed from a ring R, and $C^\infty(M)$ where M is a manifold.

Definition 1.4 (Ring Homomorphism)**.** A ring homomorphism is a map f between rings A and B such that f respects addition, multiplication, and the identity element 1, i.e. $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, and $f(1) = 1$.

Definition 1.5 (Subring)**.** A subset S of a ring A is a subring of A if A is a ring with respect to the operations' of A. Alternatively, S should be closed under addition, multiplication, and contains the identity element of A.

The commutative rings and the ring homomorphisms between them form a category **CRing**, the category of commutative rings.

Definition 1.6 (Ideal)**.** An ideal I of a ring A is a subset of A which is an additive subgroup and is such that $AI \subseteq I$.

Remark 1.7. The kernel of a ring homomorphism is always an ideal. The image of a ring homomorphism is always a subring. Ideals are usually not subrings.

The ring and the trivial subring are always ideals.

The quotient structure of a ring over an ideal is automatically a quotient group. The quotient structure then inherits a uniquely-defined multiplication from the ring and by the construction we have a ring structure. Therefore, the quotient structure is called a quotient ring. There is a natural surjective ring homomorphism from the ring into the quotient structure. The most important result on quotient ring structures is the following correspondence theorem.

Theorem 1.8 (Correspondence Theorem)**.** Given a ring R and an ideal I of R, there is a correspondence between ideals of R/I and the ideals of R that contain I.

Definition 1.9 (Zero-divisor, Integral Domain)**.** A zero-divisor x of a ring R is an element $x \in R$ such that there exists a non-zero $y \in R$ such that $xy = 0$.

A ring R is called an integral domain if R have no zero-divisors.

Remark 1.10. $\mathbb{Z}$ is an integral domain.

Definition 1.11 (Nilpotent, Reduced)**.** An element x in a ring R is called nilpotent if $x^n = 0$ for some $n > 0$. We say R is reduced if R have no nilpotent elements.

Remark 1.12. A nilpotent element is a zero-divisor whenever A is not the trivial ring.

Definition 1.13 (Divide, Unit, Inverse)**.** In a ring R, we say an element x divides another element x' if there exists some $y \in R$ such that $x' = xy$.

An element $x \in R$ is called a unit if x divides 1, that is, $xy = 1$ for some y. In this case, y is called the multiplicative inverse of x, denoted x^{-1}. Analogously, y is called the additive inverse of x if $x + y = 0$, and we denote $y = -x$.

The units of R form a multiplicative Abelian group, denoted $R^\times$.

Definition 1.14 (Principal Ideal)**.** The ideal consisting multiples rx of an element $x \in R$ is called principal, denoted (x) or Rx.

Remark 1.15. x is a unit if and only if $R = (x)$.

Definition 1.16. We say a ring R is a field if $1 \neq 0$ and every non-zero element is a unit.

Remark 1.17. Every field is an integral domain.

Remark 1.18. In **CRing**, $\mathbb{Z}$ is the initial object (zero object), the zero ring is the terminal object.

Proposition 1.19. Let R be a non-trivial ring. The following are equivalent:

1. R is a field.
2. The only ideals of R are 0 and R.
3. Every homomorphism of R into a non-zero ring S is injective.

Definition 1.20. An ideal I of a ring R is prime if $I \neq R$ and whenever $xy \in I$ we have either $x \in I$ or $y \in I$.

An ideal I of a ring R is maximal if $I \neq R$ and there is no other ideal J such that $I \subsetneq J \subsetneq R$.

An ideal I of a ring R is radical if for every $x \in R$ such that $x^n \in I$ for some n, we must have $x \in I$.

Remark 1.21. An ideal I is prime if and only if R/I is a domain.

An ideal I is maximal if and only if R/I is a field.

An ideal I is radical if and only if R/I is reduced.

Geometrically speaking, maximal ideals of a ring corresponds to (closed) points in Zariski topological space, and prime ideals of a ring corresponds to irreducible closed subsets (varieties), which relates a ring to its spectrum. We will talk about these ideas later.

Example 1.22. Every ideal of $\mathbb{Z}$ is a principal ideal, therefore of the form (m) for some $m \geq 0$. The prime ideals of $\mathbb{Z}$ are of the form (m) where m is either 0 or a prime number. The maximal ideals of $\mathbb{Z}$ are of the form (m) where m is a prime number. The radical ideals of $\mathbb{Z}$ are the principal ideals generated by the integers, i.e. (m) for any integer m.

Alternatively, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime; it is a domain if and only if n is prime or 0; it is reduced if and only if n is a product of distinct primes.

Example 1.23. For a field K, we consider $K[x]$. The maximal ideals of $K[x]$ are of the form $(f(x))$ where f is an irreducible polynomial, and the prime ideals of $K[x]$ are (0) and the maximal ideals.

Example 1.24. In $\mathbb{Z}[x]$, the prime ideals are generated by 0 and primes, and linear combinations of x and the integers. The quotient in $\mathbb{Z}[x]$ satisfies properties like $\mathbb{Z}[x]/(7) \cong \mathbb{Z}/7\mathbb{Z}[x]$ and $\mathbb{Z}[x]/(x-3) \cong \mathbb{Z}$.

In general, for any ring R, $a \in R$, and $R[x]/(x-a) \cong R$.

Example 1.25. Consider a field K, a set S and fix an arbitrary point $s \in S$. A ring of K-valued fucntions on S, including the constants in K, then maximal ideals are of the form $I = \{f \in A : f(s) = 0\}$, set of functions that vanishes at some $s \in S$.

Lemma 1.26. Let $f : A \to B$ be a ring homomorphism with prime ideal $P \subseteq B$, then $f^{-1}(P)$ is prime in A.

Remark 1.27. This is not true for maximal ideals. For example, if $f : \mathbb{Z} \to \mathbb{Q}$ is the inclusion map, then $f^{-1}((0)) = (0) \subseteq \mathbb{Z}$ is not maximal.

Theorem 1.28. Every nonzero ring A has a maximal ideal.

Proof. Appeal to Zorn's lemma. □

Corollary 1.29. For every proper ideal $\mathfrak{a}$ of ring A, there exists a maximal ideal $\mathfrak{m}$ of A that contains $\mathfrak{a}$.

Corollary 1.30. Every non-unit element of A is contained in some maximal ideal of A.

Definition 1.31 (Local Ring, Residue Field)**.** A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a local ring. In particular, we call $A/\mathfrak{m}$ the residue field of A (with respect to $\mathfrak{m}$).

Definition 1.32 (Principal Ideal Domain)**.** A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Proposition 1.33. In a PID, every non-zero prime ideal is maximal.

Definition 1.34 (Radical)**.** The radical of an ideal I in a ring R is $\sqrt{I} = \{x \in R : \exists n \in \mathbb{N}, x^n \in I\}$.

Remark 1.35. The radical of an ideal I in R is also an ideal in R. Moreover, the radical of I is the intersection of all prime ideals of R that contains I.

Example 1.36. If $f_1, \cdots, f_r$ are polynomials in $K[x_1, \cdots, x_n]$, let $V(f_1, \cdots, f_r)$ be the set of points of K^n consisting of the common vanishing set of these polynomials.

The ideal generated by the f_i's certainly also vanishes on $V(f_1, \cdots, f_r)$.

In good cases, the set of functions vanishing on $V(f_1, \cdots, f_r)$ will be exactly the ideal $(f_1, \cdots, f_r)$.

The ring $K[x_1, \cdots, x_n]/\sqrt{(f_1, \cdots, f_r)}$ consists of polynomial functions on $V(f_1, \cdots, f_r)$. Therefore, if different polynomials agree on $V(f_1, \cdots, f_r)$, then their differences vanishes in the radical ideal $\sqrt{(f_1, \cdots, f_r)}$.

Example 1.37. Consider $K[x, y]/(y, y - x^2)$. The set $V(y, y - x^2)$ is now just the parabola $y = x^2$ intersect by the set x-axis, which is the set $\{(0, 0)\}$. Note that the two curves do not intersect transversely.

Note that $K[x, y]/(y, y - x^2) = K[x]/(x^2)$. Therefore, we have a nilpotent element x. The vanishing point is now $x = 0$, and this is a fat point since it has multiplicity 2.

Definition 1.38 (Nilradical)**.** The nilradical of A is the set η of nilpotent elements in A, which is also an ideal in A.

Proposition 1.39. The nilradical is precisely the radical of the zero ideal, i.e., sometimes denoted $\sqrt{0}$, and is also precisely the intersection of all prime ideals.

Proof. $\eta \subseteq \bigcap_{P \in \mathbf{Spec}(R)} P$: if $x^m = 0$, since $0 \in P$, so $x \in P$.

$\bigcap_{P \in \mathbf{Spec}(R)} P \subseteq \eta$: let $x \in R$ be not nilpotent. Consider the set S of ideals I in R such that $x^n \notin I$ for all $n \geq 1$. It is not empty since the zero ideal is in it. For any totally ordered subset $T \subseteq S$, let $J = \bigcup_{I \in T} I$. This is also an ideal in S. By Zorn's Lemma, S has a maximal element K. It does not contain x.

Claim 1.40. K is prime.

Subproof. Suppose $a \notin K$, $b \notin K$, we want to show that $ab \notin K$. By maximality, $(a) + K$ is not in S. Therefore, $x^n \in (a) + K$ for some n. Similarly, $x^m \in (b) + K$. But now $x^{n+m} \in (ab) + K$, so $(ab) + K \notin S$, and so $ab \notin K$. ■

□

Definition 1.41. The Jacobson radical of a ring A is the intersection of all maximal ideals of the ring.

Proposition 1.42. The Jacobson ideal is precisely the set of elements $x \in A$ such that $1 - xy$ is a unit in A for all $y \in A$.

2 Zariski Topology and Spectrum

Definition 2.1 (Zariski Topology, Spectrum)**.** Let A be a ring and let X be the set of prime ideals of A. For each subset E of A, denote $V(E)$ as the set of all prime ideals of A which contain E. Note that $V(E)$ behaves like the closed sets in a topology, in particular

- Suppose $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$, where $r(\mathfrak{a})$ is the radical of $\mathfrak{a}$.
- $V(0) = X$ and $V(1) = \varnothing$.
- $V(\bigcup\limits_{i \in I} E_i) = \bigcap\limits_{i \in I} V(E_i)$ for any family of subsets $(E_i)_{i \in I}$ in A.
- $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideal $\mathfrak{a}, \mathfrak{b}$ of A.

Therefore, we call the corresponding topology on X the Zariski topology. In particular, X is called the prime spectrum, denoted $\mathbf{Spec}(A)$.

Theorem 2.2. $\mathbf{Spec}(A)$ is a topological space for any commutative ring A.

Proof. Left as an exercise. □

Example 2.3. Consider a structure $A = K[x_1, \cdots, x_n]$, with a given $(a_1, \cdots, a_n)$. Note that points are like maximal ideals, and ring of functions vanishing at a point are maximal ideals $(x_1 - a_1, \cdots, x_n - a_n)$. Therefore, points are in one-to-one correspondence with the homomorphisms from A to K.

All prime ideals of A arise as $f^{-1}(0)$ for some map from A to K a field.

There are a few common operations defined on ideals. We can see how these operations interact on the spectrum.

Example 2.4 (Operations on Ideals)**.**

- For any ideals I, J, $I + J$ is the smallest ideal containing I and J. It contains the sum of elements of I and J.

  Let S be a set of ideals in R, then $\sum\limits_{I \in S} I$ is the smallest ideal that contains every ideal in S. It consists of finite sum of elements of the ideals in S.

- IJ is the ideal generated by elements of the form xy where $x \in I$ and $y \in J$. It is essentially the set of finite sums of elements of this form.
- $I \cap J$ is the set-theoretic intersection of I and J.

Geometrically, the vanishing set of $I + J$ is the intersection of the vanishing set of I and the vanishing set of J. A smaller vanishing set corresponds to a larger ideal. In particular, taking products and intersections of ideals corresponds to taking the union of vanishing sets.

Example 2.5.

- $IJ \subseteq I \cap J$.
- Obviously IJ is not always equal to $I \cap J$. Take $I = J$ for example. One can also find examples where $IJ \neq I \cap J$ and $I \neq J$.
- Show that if $I + J = R$, then $IJ = I \cap J$.
- Show that if $I_1, \cdots, I_n$ is a set of distinct ideals with $I_j + I_j = R$ for all $i \neq j$, then the map $R \to \prod_{i=1}^{n} R/I_i$ is surjective.

Lemma 2.6. $\sqrt{IJ} = \sqrt{I \cap J}$.

Proof. Since $IJ \subseteq I \cap J$, then $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. For the other inclusion, we see that if $x^n \in I \cap J$, then x^{2n} is in IJ. □

Lemma 2.7. If $\sqrt{I} = \sqrt{J}$, then any prime ideal containing I also contains J.

Proof. Take an prime ideal P that contains I, then $\sqrt{I} \subseteq P$. Indeed, if $I \subseteq P$, then for $x \in \sqrt{I}$, $x^n \in I \subseteq P$, and so $x \in P$. Therefore, $\sqrt{J} \subseteq P$, therefore we know $J \subseteq P$. □

Definition 2.8 (Scheme)**.** A scheme is a functor $F : \mathbf{Ring} \to \mathbf{Set}$ satisfying certain conditions. It is covered by the corresponding functors $\mathbf{Hom}_{Ring}(R, -)$ and that these functors glue together to give F.

Alternatively, a scheme is a locally ringed space, locally isomorphic to an affine scheme.

An affine scheme is a topological space that comes with a sheaf of rings cooked up out of a ring.

Definition 2.9 (Affine Algebraic Variety)**.** Let K be an algebraically closed field and let $f_\alpha(x_1, \cdots, x_n) = 0$ be a set of polynomial equations in n variables with coefficients in K. The set X of all points $x = (x_1, \cdots, x_n) \in K^n$ which satisfy these equations is an affine algebraic variety.

Consider the set of all polynomials $g \in K[x_1, \cdots, x_n]$ with the property that $g(x) = 0$ for all $x \in X$. This set is an ideal $I(X)$ in the polynomial ring, and is called the ideal of the variety X. The quotient ring $P(X) = K[x_1, \cdots, x_n]/I(X)$ is the ring of polynomial functions on X, because two polynomials g, h define the same polynomial function on X if and only if $g - h$ vanishes at every point of X, that is, if and only if $g - h \in I(X)$.

Example 2.10. Recall that $\mathbf{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), \cdots\}$.

Evaluating the "function" n at the different "points" in $\mathbf{Spec}(\mathbb{Z})$ means taking the image of n in $\mathbb{Z}/(p)$, so just have a map $\mathbb{Z} \to \mathbb{Z}/(p)$ that sends n to $\bar{n}$. The vanishing set of such functions are closed in the topology. For example, take $n = 12$, then 12 vanishes at (2) and (3) in the spectrum.

(0) is the generic point, in the sense that it is "near" every point.

Example 2.11. $\mathbf{Spec}(0) = \varnothing$ and $\mathbf{Spec}(\mathbb{Q}) = \{(0)\}$, i.e. a single point. Also, $\mathbf{Spec}\mathbb{C}[x]$ is the set of ideals of the form $(x - a)$ for any $a \in \mathbb{C}$.

Example 2.12.

1. $\mathbf{Spec}(K)$ is a point for a field K.
2. $\mathbf{Spec}(\mathbb{C}[x])$ is a cofinite topology on $\mathbb{C}$ with a generic point.
3. $\mathbf{Spec}(\mathbb{R}[x])$ has real points and points corresponding to complex conjugate numbers.
4. $\mathbf{Spec}(\mathbb{C}[x, y]/(xy))$ is two copies of $\mathbf{Spec}(\mathbb{C}[x])$ glued at the origin.

We usually write points of $\mathbf{Spec}(R)$ as x, y, with corresponding prime ideals P_x, P_y.

Proposition 2.13. For $x \in \mathbf{Spec}(R)$, then $\overline{\{x\}} = V(P_x)$.

Proof. We need to show that $V(P_x)$ is contained in any closed set containing x. Suppose $y \in V(P_x)$ and $x \in V(I)$. Then $I \subseteq P_x \subseteq P_y$. □

For a point x, the singleton $\{x\}$ is just its own closure. The closed points of $\mathbf{Spec}(R)$ are given by maximal ideals.

Spec satisfies functoriality.

Lemma 2.14. For $f : R \to S$ a morphism of rings, the preimage of an ideal is an ideal.

Proof. IF I is ideal in S, $f^{-1}(I)$ is the kernel of $R \to S \to S/I$. If I is prime, then S/I is a domain. □

Theorem 2.15. Let $f : R \to S$ be a ring homomorphism, then $f^{\#} : \mathbf{Spec}(S) \to \mathbf{Spec}(R)$ given by $I \mapsto f^{-1}(I)$. Then

1. $f^{\#}$ is continuous.

2. For an ideal I in R, $\mathbf{Spec}(R/I) \to \mathbf{Spec}(R)$ is homeomorphism onto the closed subset $V(I)$.

Proof. 1. It suffices to show that the preimage of a closed set is closed. Indeed, we know $(f^{\#})^{-1}(V(I)) = V((f(I)))$, where $(f(I))$ is an ideal in S generated by $f(I)$. Now $y \in (f^{\#})^{-1}(V(I))$ if and only if $f^{\#}(y) \in V(I)$ if and only if $I \subseteq f^{-1}(P_y)$. Therefore, $f(I) \subseteq P_y$, and so $y \in V((f(I)))$. Also, if $y \in V((f(I)))$, then $(f(I)) \subseteq P_y$, but $I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(P_y)$, and so $y \in (f^{\#})^{-1}(V(I))$.

2. $\mathbf{Spec}(R/I) \cong V(I) \subseteq \mathbf{Spec}(R)$, where the isomorphism is given by $R \to R/I$. The inverse is continuous. Show image of closed set in $\mathbf{Spec}(R/I)$ is still closed in $\mathbf{Spec}(R)$. We want to show $\pi^{\#}(V(J)) = V(\pi^{-1}(J))$. Note that for $x \in V(J)$, we know $J \subseteq P_x$, so $\pi^{-1}J \subseteq \pi^{-1}P_x$, i.e. $\pi^{\#}x \in V(\pi^{-1}J)$. Therefore, we have $\pi^{\#}(V(J)) \subseteq V(\pi^{-1}(J))$. On the other hand, for $y \in V(\pi^{-1}J)$, then $\pi^{-1}J \subseteq P_y$, and as $I \subseteq \pi(P_y)$ is a prime ideal in P/I, so $y \in \pi^{\#}(V(I))$.

□

Corollary 2.16. For a ring R, $R \to R/\sqrt{0}$ induces a homeomorphism $\mathbf{Spec}(R/\sqrt{0}) \to \mathbf{Spec}(R)$.

Definition 2.17. A nonempty space X is irreducible if X is not the union of two proper closed subsets of X. (Equivalently, every pair of non-empty open sets in X intersect, or we can say every non-empty open set is dense in X.)

Proposition 2.18. $\mathbf{Spec}(R)$ is irreducible if and only if the nilradical of R is prime.

Proof. Suppose that $\sqrt{0}$ is prime and suppose that $\mathbf{Spec}(R) = V(I) = \cup V(J)$. Moreover, suppose that $\mathbf{Spec}(R) \neq V(I)$. It suffices to show that $\mathbf{Spec}(R) = V(J)$, and it suffices to show that $J \subseteq \sqrt{0}$, which is the intersection of all prime ideals of R. Note that $\mathbf{Spec}(R) \neq V(I)$ and there is some $x \in I$ that is not contained in every prime ideal. Let $j \in J$ and $V(IJ) = \mathbf{Spec}(R)$, then this implies that $xj \in IJ$ is contained in every prime ideal. Therefore, $xj \in \sqrt{0}$. But x is not contained in every prime ideal, so $x \notin \sqrt{0}$, and so $J \subseteq \sqrt{0}$. Therefore, $V(J) = \mathbf{Spec}(R)$.

In the other direction, suppose $\mathbf{Spec}(R)$ is irreducible. Now if $V(I) \cup V(J) = \mathbf{Spec}(R)$, then $V(I)$ or $V(J)$ is all of $\mathbf{Spec}(R)$. Suppose $xy \in \sqrt{0}$, and x is not nilpotent. Then $0 \subseteq (x)(y) \subseteq \sqrt{0}$, so $V((x)(y)) = \mathbf{Spec}(R)$. Therefore, $\mathbf{Spec}(R) = V(x) \cup V(y)$. Now $V(x) \neq \mathbf{Spec}(R)$, otherwise x is contained in every prime ideal and therefore nilpotent. Therefore, $\mathbf{Spec}(R) = V(y)$, and so y is in every prime ideal, so y is nilpotent. Therefore, the nilradical of R is prime. □

Remark 2.19. The closure of an irreducible is irreducible.

Every irreducible closed subset of $\mathbf{Spec}(R)$ is of the form $V(P)$.

Every prime ideal contains a minimal prime ideal.

If n is a minimal prime, then $V(n)$ is a maximal irreducible set of $\mathbf{Spec}(R)$. In particular, if prime ideals satisfy $P_1 \subseteq P_2$, then $V(P_1) \supseteq V(P_2)$.

Definition 2.20. A maximal irreducible subset of a space X is called a component of X.

Remark 2.21. Note that the nilradical is the intersection of all the elements in $\mathbf{Spec}(R)$, then $\mathbf{Spec}(R)$ is the union of its maximal irreducible subsets.

In a ring R, a closed subset in $\mathbf{Spec}(R)$ is irreducible if and only if it is the closure of a point.

Let $S \subseteq \mathbf{Spec}(R)$ be an irreducible closed subset. Now we have $S = V(I)$ for some unique radical ideal $I \subseteq R$, then we want to show that I is prime if S is irreducible. Suppose $I \neq R$, let $a, b \in R$ such that $ab \in I$. Consider $V(I + (a)), V(I + (b)) \subseteq V(I) \subseteq \mathbf{Spec}(R)$. Suppose $a, b \notin I$. Since I is radical and $I + (a)$ and $I + (b)$ are strictly larger , then $V(I + (a))$ and $V(I+(b))$ are strictly closed subset of S. Now $V(I+(a)) \cup V(I+(b)) = V((I+(a))(I+(b))) = V(I + (ab))$, and so $V(I)$ is not irreducible, contradiction. Therefore, I is prime.

3 Modules

Definition 3.1 (Module)**.** Let A be a ring. An A-module is $(M, \mu : A \times M \to M)$ where is an Abelian group and on which A acts linearly, i.e. μ linearizes rings. That is to say, μ satisfies

- $a(x + y) = ax + ay$,
- $(a + b)x = ax + bx$,
- $(ab)x = a(bx)$,
- $1x = x$

for all $a, b \in A$ and $x, y \in M$. Equivalently, M is an Abelian group with a ring homomorphism $A \to \mathbf{End}(M)$.

A mapping $f : M \to N$ is called an A-module homomorphism (or A-linear) if M, N are A-modules and $f(x + y) = f(x) + f(y)$ and $f(ax) = a \cdot f(x)$ for all $x, y \in M$ and $a \in A$.

Essentially, an R-module linearizes rings.

Remark 3.2. The set of R-module homomorphisms form an Abelian group. In particular, for a commutative ring R, $\mathbf{Hom}_R(M, N)$ is an R-module. This can be done by defining operations $f + g$ and af elementwise.

Example 3.3.

1. For a field K, a K-module is a K-vector space.
2. Free R-modules: $R = \mathbb{Z}$, the structure $\mathbb{Z} \otimes \mathbb{Z}$.
3. A $\mathbb{Z}$-module is just an Abelian group.
4. An ideal I in commutative ring R is an R-module, and R/I is an R-module.
5. A $K[x]$-module M is equivalent to a K-vector space M together with a K-linear map $M \to M$. This can be extended to $K[x_,1 \cdots, x_n]$.
6. For a topological space X, a vector bundle is a surjective map $\pi : E \to X$. The set of sections of π is a $C(X)$-module.
7. For any group G and any field K, a group ring is defined as KG. A representation of G over K is exactly a KG-module.

Definition 3.4 (Annihilator)**.** The annihilator of an A-module M is $\mathbf{Ann}_A(M) = \{a \in A : am = 0 \in M \; \forall m \in M\}$. The annihilator is an ideal of A.

Definition 3.5 (Faithful)**.** We say an A-module M is faithful if $\mathbf{Ann}_A(M) = 0$. Moreover, if $\mathbf{Ann}_A(M) = \mathfrak{a}$, then M is faithful as an $A/\mathfrak{a}$-module.

Definition 3.6. For any subset S of R-modules M, the R-module of M generated by S is

1. Intersection of all R-submodule of M containing S, or alternatively
2. Finite R-linear combinations of elements of S.

Definition 3.7 (Free Module)**.** A free A-module is a module isomorphic to an A-module of the form $\bigoplus_{i \in I} M_i$ where each $M_i \cong A$ as an A-module. Therefore, a finitely-generated free A-module is isomorphic to $A^{\oplus n} \cong A^n$. In particular, let I be a set and R is a ring. The free R-module over I, $R^{\otimes I}$ is the set of functions $f : I \to R$ such that $\{x \in I : f(x) \neq 0\}$ is finite.

General direct sum and product are usual categorical notions. Every R-module is a quotient of a free module.

Proposition 3.8. M is a finitely-generated A-module if and only if M is isomorphic to a quotient of A^n for some integer $n > 0$.

Lemma 3.9 (Nakayama)**.** Let M be a finitely-generated A-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical of A. Then $\mathfrak{a}M = M$ implies $M = 0$.

Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $K = A/\mathfrak{m}$ its residue field. Let M be a finitely-generated A-module. $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, hence is naturally an $A/\mathfrak{m}$-module, i.e., a K-vector space, and as such is finite-dimensional.

Proposition 3.10. Let $x_1, \cdots, x_n$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space, then $x_1, \cdots, x_n$ generate M.

Exact sequences are sometimes used for the presentation of modules.

Proposition 3.11. Suppose we have a sequence of A-modules

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0,$$

then the sequence is exact if and only if the following sequence is exact for every A-module N:

$$0 \to \mathbf{Hom}(M_3, N) \xrightarrow{f} \mathbf{Hom}(M_2, N) \xrightarrow{g} \mathbf{Hom}(M_1, N)$$

Alternatively, suppose we have a sequence of A-modules

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3,$$

then the sequence is exact if and only if the following sequence is exact for every A-module N:

$$0 \to \mathbf{Hom}(N, M_1) \xrightarrow{f} \mathbf{Hom}(N, M_2) \xrightarrow{g} \mathbf{Hom}(N, M_3)$$

Definition 3.12 (Free Presentation)**.** A free presentation of an R-module is an exact sequence

$$R^{\otimes J} \longrightarrow R^{\otimes I} \longrightarrow M \longrightarrow 0$$

That is, M is generated by I elements $e_i \in M$ for $i \in I$. The exactness implies that $M \cong R^{\otimes I}/\mathbf{im}(R^{\otimes J})$. In particular, if I is finite, then M is a finitely-generated module. If I and J are finite sets, then the presentation is called a finite presentation; a module is called finitely presented if it admits a finite presentation.

Lemma 3.13. Every R-module has a presentation.

Proof. Consider R-module M and choose a set of generators of M, namely I. Now there is an exact sequence

$$\ker(f) \longrightarrow R^{\otimes I} \xrightarrow{f} M \longrightarrow 0$$

Then choose generators f_j for $\ker(f)$, where $j \in J$. We now extend the sequence to

$$R^{\otimes J} \longrightarrow R^{\otimes I} \xrightarrow{f} M \longrightarrow 0$$

Note that the kernel might not be free. □

Example 3.14. Let M be the $\mathbb{Z}$-module $\mathbb{Z}\langle e_1, e_2 \mid 2e_1 = 2e_2 \rangle$, which is the cokernel of $\mathbb{Z} \to \mathbb{Z}^2$ that sends $1 \mapsto (2, -2)$.

One can show that $M \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Definition 3.15 (Projective)**.** An R-module is projective if it is a direct summand of a free module.

Example 3.16.

1. A free R-module is projective.
2. For field K, every K-module is free, and therefore projective.
3. A module M over a PID is projective if and only if it is free.

Note that $\mathbb{Q}$ is not projective over $\mathbb{Z}$ because it is not free.

Lemma 3.17. Let M be a R-module. The following are equivalent:

1. M is projective.
2. Any exact sequence $0 \longrightarrow A \longrightarrow B \underset{\curvearrowleft\, \exists s}{\xrightarrow{f}} M \longrightarrow 0$ splits.
3. For any exact diagram $\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & & & \nwarrow & \uparrow & & \\ & & & & & & M & & \end{array}$ such that $M \to C$ is R-linear, we have a lift to the map $M \to B$.

Proof. (2) $\Rightarrow$ (1): Let $R^{\otimes I} \to M \to 0$ be a set of generators for M. Let $A = \ker(f)$, then $0 \to A \to R^{\otimes I} \to M \to 0$ is exact. By (2), it splits, so $R^{\otimes I} = A \otimes M$, so M is projective.

(3) $\Rightarrow$ (2): The lift gives a splitting as desired.

(1) $\Rightarrow$ (3): exercise. □

Example 3.18. Let E be a real vector bundle over a paracompact Hausdorff space X. This space X is neither compact nor finite-dimension. Note that we can always find another vector bundle F such that $E \oplus F \cong \mathbb{R}_X^N$, which is the trivial bundle of rank N. The module of sections of the vector bundle E is projective, since $M_E \oplus M_F \cong C(X)^{\oplus N}$.

Lemma 3.19 (Snake Lemma)**.**

4 Tensor Product

Definition 4.1. An R-linear map $M \times N \to P$ of R-modules is a R-linear map in each variable.

The tensor product of R-modules is an R-module $A \otimes_R B$ equipped with a bilinear map $\otimes : A \times B \to A \times_R B$. This map satisfies the universal property. For every R-bilinear map $f : A \times B \to M$, there is a unique linear map $g : A \otimes_R B \to M$ such that $g \circ \otimes = f$.

The following lemma says that the tensor product can be obtained by quotienting certain equivalence relations out of the usual categorical product.

Lemma 4.2. The tensor product of any two R-modules A, B exists. Let M be the quotient of the free $R^{\oplus(A\times B)}$ by the submodule generated by $(a_1 + a_2) \otimes b - a_2 \otimes b - a_1 \otimes b$, $a \otimes (b_1 + b_2) - a \otimes b_1 - a \otimes b_2$, $r(a \otimes b) - ra \otimes b$, and $r(a \otimes b) - a \otimes (rb)$ for all $r \in R$, $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$.

In other words, the tensor product has the property that the A-bilinear mappings $M \times N \to P$ are in a natural one-to-one correspondence with the A-linear mappings $T \to P$, for all A-modules P. More precisely:

Proposition 4.3. Let M, N be A-modules. Then there exists a pair (T, g) consisting of an A-module T and an A-bilinear mapping $g : M \times N \to T$, with the following property:

Given any A-module P and any A-bilinear mapping $f : M \times N \to P$, there exists a unique A-linear mapping $f' : T \to P$ such that $f = f' \circ g$, i.e. every bilinear function on $M \times N$ factors through T. Moreover, if (T, g) and (T', g') are two pairs with this property, then there exists a unique isomorphism $j : T \to T'$ such that $j \circ g = g'$.

Remark 4.4. Every element of $M \otimes_R N$ is a finite sum $\sum_{i=1}^{N} r_i(m_i \otimes n_i)$, this also equals $\sum_{i=1}^{r} (rm_i) \otimes n_i$, so everything is just a sum of basis elements (not unique).

It is not true that every element is of form $m \otimes n$.

It may not be clear whether an element is zero or not in this structure.

For a noncommutative ring R, can define a tensor product of a right R-module M and a left R-module N. Now $M \otimes_R N$ is not an R-module, but it is an Abelian group.

Tensor products is a functor in each variable.

Lemma 4.5. Let $x_i \in M, y_i \in N$ such that $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Then there exists finitely generated submodules M_0 of M and N_0 of N such that $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.

Proof. $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Now $\sum(x_i, y_i) \in D$ indicates the sum is a finite sum of generators in D. Let $M_0 \subseteq M$ generated by x_i and elements of M occurs as first coordinates in the generator of D. Similarly for N_0. Now $\sum x_i \otimes y_i = 0$ as an element of $M_0 \otimes N_0$. □

Remark 4.6. Inductively, there is a multi-tensor product.

Proposition 4.7. Let M, N, P be R-modules. Then there exists unique isomorphisms that are also canonical:

- $M \otimes N \to N \otimes M$,
- $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$,
- $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$,
- $A \otimes M \to M$.

Lemma 4.8. Tensor product preserves right exact sequences. For an exact sequence

$$A \to B \to C \to 0$$

of R-modules,

$$A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

is exact.

Example 4.9. For any element $f \in R$, apply lemma to $R \xrightarrow{\cdot f} R \to R/(f) \to 0$. Get that for any R-module M, $M \xrightarrow{\cdot f} M \to M \otimes_R R/(f) \to 0$ is exact. Now $M \otimes_R R/(f) = M/(f)$.

For example, $(\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}) = \mathbb{Z} \oplus 0$.

Example 4.10. Given a ring R and R-modules M and N with a presentation for each, i.e.

$$R^{\oplus I_1} \to R^{\oplus I_0} \to M \to 0$$

and

$$R^{\oplus J_1} \to R^{\oplus J_0} \to M \to 0$$

are exact. By the result of exactness of tensor product with M, we get an exact sequence

$$M^{\oplus J_1} \to M^{\oplus J_0} \to M \otimes_R N \to 0$$

We can turn this into a presentation of $M \otimes_R N$ by considering $M \otimes_R N$ $M \otimes_R N$ as generated by $e_i \otimes f_j$ for generators e_i of M and f_j of N. The rational r_i in M produce relation $r_i \otimes f_i$ in $M \otimes_R N$. For example, $R/(a_1) \otimes R/(a_2) \cong R/(a_1. \cdots, a_2)$.

Definition 4.11. Let $f : A \to B$ be a homomorphism of rings and let N be a B-module. Then N has an A-module structure defined as follows: if $a \in A$ and $x \in N$, then ax is defined to be $f(a)x$. This A-module is said to be obtained from N by restriction of scalars. In particular, f defines in this way an A-module structure on B.

Proposition 4.12. Suppose N is finitely-generated as a B-module and that B is finitely-generated as an A-module, then N is finitely-generated as an A-module.

Note that the tensor product and the hom functor commutes well, and gives the tensor-hom adjunction.

Remark 4.13. There is a canonical isomorphism given by

$$\mathbf{Hom}(M \otimes N, P) \cong \mathbf{Hom}(M, \mathbf{Hom}(N, P)).$$

Definition 4.14. An R-module M is flat if the functor $- \otimes_R M$ is exact.

Example 4.15. $\mathbb{Z}/2\mathbb{Z}$ not flat as a $\mathbb{Z}$-module.

Any free module is flat. Moreoverally, any projective module is flat, since the summand of flat modules is flat.

Example 4.16. $\mathbb{Q}$ as $\mathbb{Z}$-module is flat but not projective. We can prove flatness by applying the following lemma.

Lemma 4.17. For an R-module M, the following are equivalent:

1. M is flat.
2. The functor $- \otimes N$ preserves exact sequences of R-modules.
3. If $f : N' \to N$ is injective, then $f \otimes 1 : N' \otimes M \to N \otimes M$ is injective.
4. If $f : N' \to N$ is injective for finitely-generated R-modules N and N', then $f \otimes 1$ is injective.

Example 4.18. For a domain R, a flat R-module is torsion-free.

For a PID R, M is flat if and only if M is torsion-free.

5 Algebra

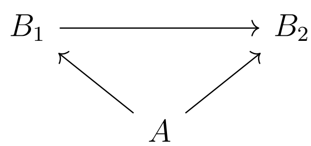
Definition 5.1. For commutative ring A, an A-algebra is a commutative ring B with a ring homomorphism $A \to B$.

Alternatively, let $f : A \to B$ be a ring homomorphism. If $a \in A$ and $b \in B$, define a product $a \cdot b = f(a)b$, then this makes B into an A-module according to the restriction of scalars. Therefore, B has an A-module structure as well as a ring structure. The structure on B is now called an A-algebra, and therefore gives the definition above.

Example 5.2. $K[x_1, \ldots, x_n]$ is a K-algebra. Any ring is a $\mathbb{Z}$-algebra in a unique way.

$M_n(K)$ is a K-algebra, and KG as group ring is a K-algebra.

Definition 5.3. An A-algebra homomorphism is a given commutative diagram



For a ring A and $n \geq 0$, the polynomial ring $A[x_1, \cdots, x_n]$ has the following universal property in the category of commutative A-algebras. That is, for any A-algebra B, we have an isomorphism between the hom set from $A[x_1, \cdots, x_n]$ to B and the functions from $\{1, \cdots, n\}$ to B.

Definition 5.4. A finitely-generated A-algebra is an A-algebra such that there exists a finite set of elements $x_1, \cdots, x_n$ in B such that every element of B can be written as a polynomial in $x_1, \cdots, x_n$ with coefficients in $f(A)$. Equivalently, there exists $a_1, \cdots, a_n \in A$ such that the evaluation homomorphism at $(a_1, \cdots, a_n)$ given by $K[x_1, \cdots, x_n] \to A$ is a surjection.

We sometimes also say such algebra is an A-algebra of finite type. In particular, we see that an A-algebra is of finite type if it is finitely-generated as an A-algebra, that is, $B \cong A[x_1, \cdots, x_n]/I$ for some ideal I.

An affine variety over a field K means $\mathbf{Spec}(R)$, where R is a domain of finite type over K. Note that since R is a domain, then the spectrum is irreducible.

If B is an A-algebra, then there is a functor from the category of B-modules to the category of A-modules, given by $M \mapsto M$, namely the restriction of scalars. (If $f : A \to B$ is the structure homomorphism given by $aM = f(a) \cdot M$.) Using the tensor product, we can define the extension of scalars as a functor from A-modules to B-modules, given by $M \mapsto M \otimes_A B$. Now B is an A-module by multiplication. $M \otimes_A B$ has the module structure, and given by $b_1(m \otimes b_2) = m \otimes (b_1 b_2)$.

Example 5.5. Note that $A^{\oplus I} \otimes_A B \cong B^{\oplus I}$. More generally, the extension of scalars with given presentation to the B-module with same presentation.

Example 5.6. If $M \cong \langle e_1, e_2 \mid 2e_1 = 2e_2 \rangle$, then $M \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then we know $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \langle e_1, e_2 \mid 2e_1 = 2e_2 \rangle \cong \mathbb{Q}e_1$, it is a one-dimensional $\mathbb{Q}$-vector space, i.e. can solve for e_2 over $\mathbb{Q}$.

Also, $M \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \langle e_1, e_2 \mid 2e_1 = 2e_2 \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Definition 5.7. An A-algebra B is flat if B is flat as an A-module.

An R-module determines vector spaces over all fields. We have $\text{Frac}(R/p)$ via tensor product for prime p in R.

Example 5.8. $\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ has dimension 1 in most places, dimension 2 at $\mathbb{Z}/7\mathbb{Z}$, "like a one-dimensional bundle everywhere except 7".

6 Rings and Modules of Fractions

Definition 6.1. Let A be a commutative ring, S be a multiplicatively closed subset (i.e., $1 \in S$, and closed under multiplication). We get a localization $A[S^{-1}]$, sometimes denoted $S^{-1}A$, in which the elements of A are invertible.

Theorem 6.2. We can define $A[S^{-1}]$ such that there is an $f : A \to A[S^{-1}]$ such that

1. For each $s \in S$, $f(s)$ is invertible.
2. $A[S^{-1}]$ is universal with the property: for any $g : A \to B$ with $g(s)$ invertible for all $s \in S$, then there is a unique map $h : A[S^{-1}] \to B$ such that $h \circ f = g$.

Example 6.3. For a domain A, $S = A \backslash \{0\}$ is multiplicatively closed $A[S^{-1}]$ is the fractional field of A.

For a domain A and S a multiplicative set without 0, then there is a map from A to $A[S^{-1}]$, and so $A \subseteq A[S^{-1}] \subseteq \text{Frac}(A)$.

If $0 \in S$, then $A[S^{-1}]$ is the zero ring.

For any ring A, if $f \in A$, then $A[\frac{1}{f}]$ is the localization with $S = \{1, f, f^2, \cdots\}$. This is the set of regular functions on the open set $\{f \neq 0\} \subseteq \textbf{Spec}(A)$.

The ring $S^{-1}A$ is sometimes called the ring of fractions of A with respect to S, and satisfies the following universal property.

Proposition 6.4. Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.

The ring $S^{-1}A$ and the homomorphism $f : A \to S^{-1}A$ have the following properties:

1. $s \in S$ implies $f(s)$ is a unit in $S^{-1}A$.
2. $f(a) = 0$ implies $as = 0$ for some $s \in S$.
3. Every element of $S^{-1}A$ is of the form $f(a)f(s)^{-1}$ for some $a \in A$ and some $s \in S$.

Conversely, these three conditions determine the ring $S^{-1}A$ up to isomorphism.

Corollary 6.5. If $g; A \to B$ is a ring homomorphism such that

1. $s \in S$ implies $g(s)$ is a unit in B.
2. $g(a) = 0$ implies $as = 0$ for some $s \in S$.
3. Every element of B is of the form $g(a)g(s)^{-1}$, then there existsa unique isomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.

Example 6.6. $\mathbf{Spec}\mathbb{Z}[\frac{1}{5}] = V(5)^c$ in the spectrum. Now $\mathbb{Z}[\frac{1}{5}]$ has maps to $\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Q}$, but not $\mathbb{Z}/5$.

Remark 6.7. Let p be a prime ideal of A, we define $A_p = A[S^{-1}]$ where $S = R\backslash p$. Here S is multiplicatively closed when p is prime. This is the localization of A at p.

Example 6.8. For example $\mathbb{Z}_{(5)}$ is the set of rationals where $b \not\equiv 0 \pmod 5$. This is essentially the germs of regular functions at 5.

$K[x, x^{-1}] = K[x][\frac{1}{x}]$ is the set of elements of the form $\frac{f}{x^r}$ with $f \in R[x]$ and $r \geq 0$. This is the ring of Laurent polynomials over K. Note that this is not a field. Moreover, this is the set of functions on affine line minus the origin.

$\mathbb{C}[x]_{(x)}$ is the set of rational functions defined at the origin.

Theorem 6.9. Let S be a multiplicative closed set of a ring A. Then the prime ideals in $A[S^{-1}]$ are in one-to-one correspondence with prime ideals $p \subseteq A$ such that $p \cap S = \varnothing$.

Proposition 6.10. S^{-1} as an operation is exact.

Example 6.11.
1. $\mathbf{Spec}(A[\frac{1}{f}]) = \{p \in \mathbf{Spec}(A) \mid f \notin p\}$, here $S = \{1, f, \cdots\}$ and $S \cap P = \varnothing$.
2. $\mathbf{Spec}(A_p) = \{q \in \mathbf{Spec}(A) \mid q \subseteq p\}$. They are in one-to-one correspondence with irreducible closed subsets of $\mathbf{Spec}(A)$ containing $V(p)$. Here $S = A\backslash p$ and $S \cap p = \varnothing$.

Proposition 6.12. Let M be an A-module. Then $S^{-1}A$-modules $S^{-1}M$ and $S^{-1}A \otimes_A M$ are isomorphic. More precisely, there exists a unique isomorphism $f : S^{-1}A \otimes_A M \to S^{-1}M$ given by $f(\frac{a}{s} \otimes m) = \frac{am}{s}$ for all $a \in A, m \in M, s \in S$.

Corollary 6.13. $S^{-1}A$ is a flat A-module.

Definition 6.14. A ring A is local if it has exactly one maximal ideal m. For a local ring A, the field A/m is called the residue field of A.

Example 6.15. A field is local.

Lemma 6.16. A ring A is local if and only if the non-units of A form an ideal of A.

Proof. ($\Rightarrow$): Let A be a local ring with maximal ideal m, then the elements in m are not units. If $a \notin m$, a must be a unit. If not, $(a) \neq R$, so (a) is contained in a maximal ideal, so $(a) \subseteq m$, and so $a \in m$, which means a is not a unit, contradiction.

($\Leftarrow$): Let A be any ring where non-units form an ideal I. Obviously $1 \in I$ and if $I \subsetneq J$, then J contains a unit, then $J = A$, and I is maximal.

We now show that I is the unique maximal ideal. If K is another maximal ideal, then $K \not\subseteq I$, but then K would have a unit, contradiction. □

Example 6.17. The power series ring $A = K[[x_1, \cdots, x_n]]$ is local since the non-units are exactly the elements with constant term 0, and forms an ideal. Moreover, $A/m = K$ in this case.

Theorem 6.18. For p a prime ideal in A, then A_p is local.

Proof. The unique maximal ideal is $m = pA_p$, corresponding to p. □

Remark 6.19. The residue field of A_p is $\mathrm{Frac}(A/p)$. For example, $\mathbb{Z}_{(p)}$ has residue field $\mathbb{Z}/p$.

$\mathbb{C}[x]_{(x)}$ is a local ring with residue field $\mathbb{C}$.

Example 6.20. Consider $\mathbb{C}[x, y]_{(x)}$, a local ring. The residue field is $\mathrm{Frac}(\mathbb{C}[y]) = \mathbb{C}(y)$.

A rational function f on $\mathbb{C}^2$ is in $\mathbb{C}[x, y]_{(x)}$ if it is of the form $\frac{g}{h}$ where $g, h \in \mathbb{C}[x, y]$, and $h \notin (x)$, which means h is not identically zero on y-axis. Therefore, f is defined on most of y-axis.

For example, $\frac{1}{1+y}$ has pole at $(0, -1)$, but it is still in $\mathbb{C}[x, y]_{(x)}$. Now there is a map $\mathbb{C}[x, y]_{(x)} \to \mathbb{C}(y)$ means restriction to the y-axis.

Proposition 6.21. Let M be an A-module, then the following are equivalent:

1. $M = 0$,

2. $M_p = 0$ for all prime ideals p of A,

3. $M_m = 0$ for all maximal ideals m of A.

Proposition 6.22. Let $\varphi : M \to N$ be an A-module homomorphism, then the following are equivalent:

1. φ is injective,

2. $\varphi_p : M_p \to N_p$ is injective for all prime ideals p,

3. $\varphi_p : M_m \to N_m$ is injective for all maximal ideals m.

Remark 6.23. Similar results hold on surjective maps.

Proposition 6.24. Let M be an A-module, then the following are equivalent:

1. M is a flat A-module,

2. M_p is a flat A_p-module for all prime ideals p.

3. M_m is a flat A_m-module for all maximal ideals m.

For a prime ideal $p \subseteq R$, the field $\mathrm{Frac}(R/p)$ is called the residue field of the ring R at p.

For an R-module M, we have an isomorphism $M_p \cong M \otimes_R R_p$, and call this the stalk of M at p, and $M \otimes_R \mathrm{Frac}(R/p)$ is called the fiber of M at p.

Remark 6.25. For an R-module M and ideal $I \subseteq R$, $M \otimes R/I \cong M/IM$. In other words,

$$(0 \to I \to R \to R/I \to 0) \otimes_R M$$

is exact, i.e.

$$0 \to I \otimes_R M \to M \to M \otimes_R (R/I) \to 0$$

is exact, and so $M \otimes R/I \cong M/IM$.

Note that for $M = 0$, it is sufficient to show that $M_p = 0$ for all prime ideal p. Note that this is only true for stalks but not fibers.

Example 6.26. Let $R = \mathbb{Z}$, then there are R-modules M with $M \neq 0$ but such that $M \otimes_{\mathbb{Z}} \mathbb{Z}/p = 0$.

Similarly, we have $R = \mathbb{Q}$ as an example.

Note that there is a $\mathbb{Z}$-module $M \neq 0$ but all its fibers at prime ideals are 0, so $M/pM = 0$ and $M \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, as every element in $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is torsion: $M \otimes_{\mathbb{Z}} \mathbb{Q} = M_{(0)}$.

Also consider $M = \mathbb{Q}/\mathbb{Z}$ identifiable with group of roots of unity.

Lemma 6.27 (Nakayama)**.** If R is a local ring, and M is a finitely-generated R-module, and m is a maximal ideal of R. If $M \otimes_R R/m = 0$, then $M = 0$.

Proof. We have $M \otimes_R R/m \cong M/mM$, so if $M \otimes_R R/m = 0$, then $M = mM$. Let $x_1, \cdots, x_n$ be a (minimal) finite set of elements generating M.

Suppose $M \neq 0$, then $x_n \in M = mM$, so we have $x_n = a_1 x_1 + \cdots + a_n x_n$ for $a_i \in m$, and now

$$(1 - a_n)x_n = a_1 x_+ \cdots + a_{n-1}x_{n-1},$$

but $1 - a_n$ is a unit, and because it maps to 1 in R/m so $1 - a_n$ is not in m, and R is a local ring, so x_n is the linear combination of $x_1, \cdots, x_{n-1}$. But now we have a contradiction because $n - 1$ elements can also generate the same set. □

Proposition 6.28. For any commutative ring R (not necessarily local), if M is a finitely-generated R-module, then $M = 0$ if and only if $M \otimes R/m = 0$ for every maximal ideal $m \in R$, if and only if $M_m = 0$ for every maximal ideal m.

Corollary 6.29. Let M be a finitely-generated module over a local ring R, then elements $x_1, \cdots, x_n \in M$ generate M as an R-module if and only if the images of $x_1, \cdots, x_n$ in $M \otimes_R R/m$ span the vector space.

Proof. If $x_1, \cdots, x_n$ generate M as an R-module, then the map $R^{\oplus n} \to M$ is onto, so the associated map $(R/m)^{\otimes n} \to M \otimes_R R/m$ is onto.

Conversely, suppose $x_1, \cdots, x_n \in M$ span $M \otimes_R R/m = M/mM$. Define Q as the cokernel of $R^{\oplus n} \to M \to Q \to 0$, the surjection $M \to Q \to 0$ gives a surjection $M/mM \to Q/mQ$ by tensoring R/m since $x_1, \cdots, x_n$ map to zero, then they map to zero in Q/mQ. We know $x_1, \cdots, x_n$ span M/mM, so they span Q/mQ, and $Q/mQ = 0$, then $Q = 0$ by Nakayama Lemma. □

Example 6.30. Q is a module over local ring $\mathbb{Z}_{(2)}$ and $Q/2Q = 0$ but $Q \neq 0$. Note that Nakayama lemma doesn't work because the module M is not finitely-generated.

7 Noetherian Rings

Noetherian rings is a large category of rings, including all finitely-generated algebras over a field.

Definition 7.1. A ring R is Noetherian if every increasing sequence of ideals eventually terminates, known as the ascending chain condition.

A ring R is Artinian if it satisfies the descending chain condition, i.e. every decreasing sequence of ideals eventually terminates.

Lemma 7.2. For any ring R, the following are equivalent:

1. R is Noetherian.

2. Every ideal in R is finitely-generated.

Proof. ($\Rightarrow$): Suppose R satisfies ACC, $I \subseteq R$ is a non-finitely-generated ideal, then $I \neq 0$ so we can pick $x_1 \in I$ and $(x_1 \subsetneq I$, and $x_2 \in i \backslash (x_1)$, and so on, then we get an ascending chain $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$.

($\Leftarrow$): Suppose all ideals are finitely-generated and consider $I_1 \subseteq I_2 \subseteq \cdots$, then $J = \bigcup_{i=1}^{\infty} I_n$ is an ideal, and J is finitely-generated, then $I_N = J$, so ACC condition satisfies. □

Example 7.3. 1. Fields are Noetherian and Artinian.

2. $\mathbb{Z}$ is Neotherian but not Artinian.

3. Every Artinian ring is Noetherian.

Note that if R is domain, then the fractional field of R is Noetherian. But a subring of a Noetherian ring need not be Noetherian.

Lemma 7.4. Any quotient ring R/I of a Noetherian ring R is Noetherian. Similar fact holds for Artinian rings.

Proof. Follows from the correspondence of ideals in R/I with those in R containing I. □

Definition 7.5. An R-module M satisfies ACC for R-submofules if every increasing sequence of R-submodules terminates. In particular, R is Noetherian if and only if R as an R-module satisfies ACC for R-submodules.

Lemma 7.6. A short exact sequence of R-modules $0 \to A \to B \to C \to 0$ has B satisfies ACC for R-submodules if and only if A and C satisfies ACC for R-submodules.

Proof. ($\Rightarrow$): Note that submodules of A are also submodules of B, and similarly submodules of C are also submodules of B.

($\Leftarrow$): Let $M_1 \subseteq M_2 \subseteq \cdots$ be any sequence of submodules of B. Now the intersections $M_1 \cap A \subseteq M_2 \cap A \subseteq \cdots$ terminates, and so there exists s such that $M_s \cap A = M_{s+1} \cap A$ by the ACC condition for A, and now we know that $M_1/M_1 \cap A \subseteq M_2/M_2 \cap A \subseteq \cdots$ terminates at some t by the ascending chain condition. Let N be the maximal of s and t, then we know the chain terminates at such t. □

Theorem 7.7. Let M be a finitely-generated module over Noetherian ring R. Then every R-submodule of M is finitely-generated and M satisfies ACC.

Proof. Let us show M satisfies ACC, then finitely-generated follows from the same argument as for ideals. Since M is finitely-generated as an R-module, then there is $n \in \mathbb{N}$ such that $R^{\oplus n} \twoheadrightarrow M$. It is enough to show that $R^{\oplus n}$ satisfies ACC, which holds by building it through exact sequences by induction from R itself, which satisfies ACC as a R-module. □

Lemma 7.8. The localization of a Noetherian ring is Noetherian.

Proof. Any ideal $I \subseteq R[S^{-1}]$ can be written as $JR[S^{-1}]$ for some ideal J in R, note that J does not have to be unique. □

Theorem 7.9 (Hilbert Basis Theorem)**.** If R is Noetherian, $R[x]$ is also Noetherian.

Proof. We will show that every $I \subseteq R[x]$ is finitely-generated. For each $j \geq 0$, define $I_j = \{a \in R : \text{ there exists an element of } I \text{ with degree at most } j\}$. Now I_j is an ideal. Moreover, $I_0 \subseteq I_1 \subseteq \cdots \subseteq R$ with multiplication by x, then this process terminates, so there exists some N such that $I_N = I_{N+1} = \cdots$, and since R is Noetherian, then each I_j is finitely-generated, so $I_j = (\{f_{j,k}\})$ for $j = 0, \cdots, N$. By definition of I_j, can choose $g_{j,k} \in I$ with degree of $g_{j,k}$ at most j, and the coefficients of x^j in $g_{j,k}$ is $f_{j,k}$. It suffices to prove the following claim:

Claim 7.10. These elements generate I in $R[x]$.

We can use induction to prove this, on degree of elements in I, so it suffices to show that for any $h \in I$ of degree d, we can find a $R[x]$-linear combination of $g_{j,k}$'s such that h subtracting the linear combination has degree less than d. This means we can eventually get down to zero. Just look at the leading coefficient a of h, it is in I_d, so if $0 \leq d \leq N$, then a is a R-linear combination of $f_{j,k}$, so it form the corresponding linear combination of $g_{j,k}$. If $d > N$, then $a \in I_d = I_N$ so a is a R-linear combination of $f_{N,k}$, then $h - x^{d-N} \times$ corresponding linear combination of $g_{N,k}$ is of lower degree. □

Corollary 7.11. $K[x_1, \cdots, x_n]$ is Noetherian.

Remark 7.12. Every ideal in $K[x]$ is a principal ideal, but there is no upper bound for the number of generators required in $K[x, y]/$.

Corollary 7.13. Let R be a Noetherian ring, and A is an R-algebra of finite type. Then A is Notherian. In particular, $K[x_1, \cdots, x_n]/I$ is Noetherian.

Example 7.14.

1. $K[x]_{(x)}$, being a localization of $K[x]$, is Noetherian. But if K is infinite, then $K[x]_{(x)}$ is not finitely-generated over $K[x]$ as an algebra.
2. If R is Noetherian, so is $R[[x]]$.

3. Let $U(D)$ be the set of holomorphic functions f on open disk $D \subseteq \mathbb{C}$ is not Noetherian, despite being a subring of $\mathbb{C}[[x]]$.

   Indeed, pick infinite set of points in D, given by $\{z_1, z_2, \cdots\}$, and consider the ideals of functions vanishing on $\{z_1, \cdots\}$, $\{z_2, \cdots\}$, $\{z_3, \cdots\}$, $\cdots$.

4. $\mathbb{Z}$ is Noetherian, not an algebra over a field.

8 Primary Decomposition

Recall that commutative rings do not always admit a unique factorization of ideals, only UFDs do. We now look at a generalized form of unique factorization of ideals.

Definition 8.1. An ideal p in a ring A is primary if $p \neq A$ and $xy \in p$ implies either $x \in p$ or $y^n \in p$ for some $n > 0$.

Equivalently, p is primary if and only if $A/p \neq 0$ and every zero-divisor in A/p is nilpotent.

Remark 8.2. A prime ideal in a ring A is in some sense a generalization of a prime number. The corresponding generalization of a power of a prime number is a primary ideal.

Obviously, every prime ideal is primary.

Proposition 8.3. Let p be a primary ideal in ring A, then $\text{rad}(p)$ is the smallest prime ideal containing p.

Proposition 8.4. If $\text{rad}(a)$ is a maximal ideal, then a is a primary ideal. In particular, the powers of a maximal ideal m are m-primary.

We try to study presentations of an ideal as an intersection of primary ideals.

Lemma 8.5. The intersection of finitely many p-primary ideals is p-primary.

Lemma 8.6. Let q be p-primary, and $x \in A$. Then

1. if $x \in q$, then $q/(x) = (1)$.

2. if $x \notin q$, then $q/(x)$ is p-primary, and therefore $\text{rad}(q/(x)) = p$.

3. if $x \notin p$, then $q/(x) = q$.

Definition 8.7. A primary decomposition of an ideal a in A is an expression of a as a finite intersection of primary ideals, i.e., $a = \bigcap_{i=1}^{n} q_i$. If moreover we have $\text{rad}(q_i)$ are all distinct and that $q_i \not\supseteq \bigcap_{j \neq i} q_j$ for all $1 \leq i \leq n$, then the primary decomposition given above is said to be minimal.

We say a is decomposable if it has a primary decomposition.

Theorem 8.8 (First Uniqueness Theorem)**.** Let a be decomposable and let $a = \bigcap_{i=1}^{n} q_i$ be a minimal primary decomposition. Let $p_i = \text{rad}(q_i)$ for all $1 \leq i \leq n$, then p_i's are precisely the prime ideals which occur in the set of ideals $\text{rad}(a/(x))$ for $x \in A$, and hence are independent of the particular decomposition of a.

Remark 8.9. The prime ideals p_i's are said to be associated with a. Therefore, a is primary if and only if it has a unique associated prime ideal.

The minimal elements of $\{p_1, \cdots, p_n\}$ are called minimal prime ideals belonging to a.

Proposition 8.10. Let a be a decomposable ideal, then any prime ideal $p \supseteq a$ contains a minimal prime ideal belonging to a, and thus the minimal prime ideals of a are precisely the minimal elements in the set of all prime ideals containing a.

Proposition 8.11. Let a be decomposable, and suppose $a = \bigcap_{i=1}^{n} q_i$ is a minimal prime decomposition, and define $p_i = \text{rad}(q_i)$. Now $\bigcup_{i=1}^{n} p_i = \{x \in A : a/(x) \neq a\}$.

Theorem 8.12 (Second Uniqueness Theorem)**.** Let a be decomposable and suppose $a = \bigcap_{i=1}^{n} q_i$ is a minimal prime decomposition, let $\{p_{i_1}, \cdots, p_{i_n}\}$ be a minimal set of prime ideals of a, then $q_{i_1}, \cdots, q_{i_m}$ is independent of the decomposition.

Corollary 8.13. The minimal prime components (i.e., the primary components corresponding to minimal prime ideals) are uniquely determined by a.

We now study the decomposition of $\textbf{Spec}(R)$ in particular.

Theorem 8.14. Let R be Noetherian, then $X = \textbf{Spec}(R)$ can be written as $X = x_1 \cup \cdots \cup x_m$ with each x_i an irreducible subset, and no $x_i \subseteq x_j$ for $i \neq j$. Moreover, this decomposition is unique up to ordering of x_i's.

Proof. Any closed set in $\textbf{Spec}(R)$ is of the form $V(I)$. There is an one-to-one correspondence: $V(I)$ sends maximal ideals to closed points, sends prime ideals to irreducible closed subsets, and send radical ideals to closed subsets.

The correspondence makes the above equivalent to the following theorem. □

Theorem 8.15. Let I be an ideal of a Noetherian ring. Then I satisfies $\textbf{rad}(I) = P_1 \cap \cdots P_m$ such that P_i contains I and $P_i \subsetneq P_j$ if $i \neq j$. This decomposition is unique up to reordering of ideals.

Proof. Existence: since A is Noetherian, there is no infinite strictly descending chain of closed subsets of $\mathbf{Spec}(R)$. If X cannot be written as in the theorem, $X \neq \varnothing$ and X is not irreducible, so we can write $X = X_1 \cup Y_1$ and by induction we get an infinite chain of closed subsets, contradiction. Thus, $X = X_1 \cup \cdots \cup X_m$.

Each of the X_i's is called an irreducible component of X. □

Any subset of $\mathbb{C}^n$ defined by any collection of polynomials f_i's has only finitely many irreducible components. Note that this does not work for analytic functions, like trigonometric functions.

$\mathbb{C}^n$ is the set of closed points in $\mathbf{Spec}(\mathbb{C}[x_1, \cdots, x_n])$. In a Noetherian ring R, a radical ideal I is the intersection $I = P_1 \cap \cdots \cap P_r$ of finitely many prime ideals with the corresponding irreducible closed sets $V(I) = V(P_1) \cup \cdots \cup V(P_r)$.

Example 8.16. We can prove that every prime ideal has a minimal prime ideal containing in it. That means for $I \subseteq P$, we have $V(I) \supseteq V(P)$ is an irreducible component of $V(I)$.

Example 8.17. What are the ideals $I \subseteq \mathbb{C}[x, y]$ whose radical is (x, y)? We will have $I \subseteq (x, y)$. We can show that $(x, y)^N \subseteq I \subseteq (x, y)$. Here $(x, y)^N = (x^N, x^{N-1}y, \cdots, xy^{N-1}, y^N$.

Example 8.18. Let $N \geq 1$, and let V be a $\mathbb{C}$-linear subspace of $\mathbb{C}\{x^N, x^{N-1}y, \cdots, y^N\} \cong \mathbb{C}^{N+1}$ and let $I = V + (x, y)^{N+1}$, then I is an ideal with $rad(I) = (x, y)$ but for distinct V's we get distinct I's.

Theorem 8.19. For any ideal I in a Noetherian ring, there is an N such that $rad(I)^N \subseteq I \subseteq rad(I)$.

Proof. It suffices to show the first inclusion. For any $x \in rad(I)$ there is a positive integer N with $x^n \in I$ and since R is Noetherian, then $rad(I) = (x_1, \cdots, x_m)$. We can choose N_0 such that $x_i^{N_0} \in I$ for $i = 1, \cdots, m$. Take $N = mN_0$ so any product of N of the generators of $rad(I)$ (with repetition allowed) is in I, because $rad(I)^N$ is generated by such products. □

Lemma 8.20. Let M be a nonzero module over a Noetherian ring, then there is an element $x \in M$ with $x \neq 0$ and $Ann_R(x)$ as a prime ideal.

Proof. Consider the poset of all ideals in R of the form $Ann_R(x)$ for $x \in M$ and $x \neq 0$. By Zorn's lemma, we can show that S has a maximal element. Note that $S \neq \varnothing$ since there is some $x \neq 0$in M. For a nonempty totally ordered set $C \neq \varnothing$, we can show that there is an upper bound, which is contained in the set. If not, we can choose $I_1 \subsetneq I_2 \subsetneq \cdots$ in C, contradiction. By Zorn's lemma, poset has maximal $I = Ann_R(x_0)$ with $0 \neq x_0 \in M$. We claim that I is prime. Note that $1 \notin I$ since $1 \cdot x_0 = x_0 \neq 0$. Suppose $a, b \in R$ with $ab \in I$

and $a, b \notin I$. Then $abx_0 = 0$ but $ax_0 \neq 0$, so $J = Ann_R(ax_0)$ contains the strictly smaller ideal I (since $b \in J$), contradicting the maximality of I. □

Theorem 8.21. Let M be a finitely-generated module over a Noetherian ring R, then there is a finite sequence of R-submodules

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r = M$$

such that each quotient $M_i/M_{i-1} \cong R/p_i$, for $p_i \subseteq R$ prime ideals.

Proof. If $M = 0$ then we are done.

If $M \neq 0$, find x as in the lemma above, so $Ann_R(x) = p_1$ prime, then $M_1 = R \cdot x \subseteq M$ satisfies $M_1 \cong R/p_1$. If this quotient is not 0, then we can repeat the process and find p_2, p_3, and so on, that satisfies the isomorphism relation. If this process do not stop, we have a contradiction because we then have infinite ascending submodule chain. □

Example 8.22. This decomposition is not unique. Take $R = \mathbb{Z}$ and let $M = \mathbb{Z}$, then $\mathbb{Z}$ is already $\mathbb{Z}/(0)$ or $0 = M_0 \subseteq M_1 \subseteq M_2 = M$ for $M_1 = 2\mathbb{Z}$.

Definition 8.23. The support of R/p is the set $\{I \in \operatorname{Spec}(R) \mid (R/p)_I \neq 0\}$, which is equivalent to the set $V(P) \subseteq \mathbf{Spec}(R)$.

Also, if $0 \to A \to B \to C \to 0$ is an exact sequence of R-modules, then the support of B is the union of support of A and of C over R. This is because the localization is exact.

Example 8.24. Suppose $R = \mathbb{Z}$ and $M = \mathbb{Z}$. M is of the form $\binom{\mathbb{Z}/2\mathbb{Z}}{\mathbb{Z}}$ where the notation means M is an extension, i.e. there is an exact sequence $0 \to \mathbb{Z} \to M \to \mathbb{Z}/2\mathbb{Z} \to 0$. However, this extension is not unique.

The support of M over $\mathbb{Z}$ is just $\mathbf{Spec}(\mathbb{Z})$.

9 Homological Algebra

Definition 9.1 (Chain Homotopy)**.** A chain homotopy F between two chains $f, g : M. \to N.$ is a collection of maps $F : M_i \to N_{i+1}$ such that $dF + Fd = g - f$. If such homotopy exists, we write $f \sim g$.

Note that if $f \sim g$, then $f. = g.$ as two maps between homology groups: $H_i(M.) \to H_i(N.)$.

Definition 9.2. Suppose $f : M. \to N.$ is a chain map for which $g : N_* \to M_*$ exists such that $fg \sim 1_{M_*}$ and $gf \sim 1_{N_*}$. Then we say f and g is a chain homotopy equivalence, and induces an isomorphism on homology groups.

Remark 9.3. Every R-module has a (non-unique) resolution in fact a free module.

Example 9.4. For any ring R, any non-zero-divisor $f \in R$, the R-module $R/(f)$ has a projective resolution of length 1, i.e.

$$0 \to R \xrightarrow{f} R \to R/(f) \to 0$$

and given by

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & 0 & \longrightarrow & 0 \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

This chain map induces a homology, but not a chain homotopy equivalence unless M is projective.

Lemma 9.5. Any two projective resolution $P.$ and $Q.$ are chain homotopy equivalent.

Definition 9.6 (Derived Functor)**.** Let $F : R\text{-}\mathbf{Mod} \to S\text{-}\mathbf{Mod}$ be a right exact additive functor (for example, the tensor functor $M \mapsto M \otimes_R S$ given by a ring homomorphism $R \to S$).

The (left) derived functors of F are a sequence of functors $F_i : R\text{-}\mathbf{Mod} \to S\text{-}\mathbf{Mod}$ given an R-module M. Choose $P. \to M$. Let $F_i(M) = H_i(F(P.))$ for $i \geq 0$. Note that $F_0(M) = F(M)$.

This gives a correspondence between R-modules $\cdots \to P_2 \to P_1 \to P_0 \to 0$ and S-modules $F(P_2) \to F(P_1) \to F(P_0) \to 0$.

For commutative ring R, and M and N are R-modules.

$\mathbf{Tor}_i^R(M, N)$ is the ith derived functor of $M \mapsto M \otimes_R N$ for a fixed R-module N (for commutative rings $\mathbf{Tor}_i^R(M, N) = \mathrm{Tor}_i^R(N, M)$.

If $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of R-modules, then there is a corresponding long exact sequence

$$\mathbf{Tor}_1^R(M_1, N) \to \mathbf{Tor}_1^R(M_2, N) \to \mathbf{Tor}_1^R(M_3, N) \to M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes_R N \to 0$$

Note that**Tor** is a homology type functor, which is why it has the subscript.

To show that the left derived functors are well-defined, use the fact that any two resolutions $P.$ and $Q.$ of M are chain homotopy equivalent and the fact that chain homotopies are preserved by additive functors. Therefore, we have a chain homotopy equivalence $F(P.) \to F(Q.)$.

Example 9.7 (Computations with **Tor**)**.** As for any derived functor, $\mathbf{Tor}_0^R(M,N) \cong M \otimes_R N$.

1. If M is projective, $\mathbf{Tor}_i^R(M,N) = 0$ for $i > 0$.
2. If N is flat, $\mathbf{Tor}_i^R(M, N = 0$ for $i > 0$.
3. For $f \in R$ not a zero divisor, then

$$\mathbf{Tor}_i^R(R/(f), N) = \begin{cases} 0, & i > 1 \\ N/fN, & i = 0 \\ N[f] = \{x \in N, fx = 0\}, & i = 1 \end{cases}$$

Use complex $0 \to R \xrightarrow{f}\to R \to R/(f) \to 0$ and the tensor functor $- \otimes_R N$ on $0 \to N \xrightarrow{f} N \to 0$. Therefore, **Tor** is related to torsion.

Example 9.8. **Ext** is a cohomology-like functor, hence superscript.

$\mathbf{Ext}_R^i(M,N)$ are the derived functors $\mathbf{Hom}_R(\cdot, N) : R\mathbf{Mod} \to (R\text{-}\mathbf{Mod})^{\mathrm{op}}$, a contravariant functor.

To compute, let $P. \to M$ be a projective resolution, the $\mathbf{Ext}_R^*(M,N)$ is the cohomology of the cochain complex

$$0 \to \mathbf{Hom}_R(P_0, N) \to \mathbf{Hom}_R(P_1, N) \to \cdots$$

We say this is a cochain because the numbering is ascending.

By computation, we always have $\mathbf{Ext}_R^0(M,N) \cong \mathbf{Hom}_R(M,N)$.

1. If M is projective, $\mathbf{Ext}_R^i(M,N) = \mathbf{Hom}_R(M,N)$ with $i = 0$ and 0 if $i > 0$.
2. For $f \in R$, a non-zero-divisor, then using $0 \to R \xrightarrow{f} R \to 0$ and $0 \to N \xrightarrow{f} N \to 0$, we have

$$\mathbf{Ext}_R^i(R/(f), N) = \begin{cases} 0, & i > 1 \\ N[f], & i = 0 \\ N/fN, & i = 1 \end{cases}$$

where $N[f] = \{x \in N fx = 0\}$. Therefore, this is analogous to Poincare duality. We have $H_i(S^{-1} \cong H^{i-1}(S^1)$.

Remark 9.9 (General result on derived functor)**.** Given right exact $F : (R\text{-}\mathbf{Mod}) \to (S\text{-}\mathbf{Mod})$ and additigve. If $0 \to A \to B \to C$ is exact, we get a long exact sequence

$$\cdots \to F_2C \to F_1A \to F_1B \to F_1C \to F_0A \to F_0B \to F_0C \to 0$$

which follows from snake lemma.

Example 9.10. If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence, get long exact sequences

$$\cdots \to \mathbf{Tor}^R(M_2, N) \to \mathbf{Tor}_1^R(M_3, N) \to M_1 \otimes_R N \to M_2 \otimes_R N \to M_3 \otimes_R N \to 0$$

and

$$0 \to \mathbf{Hom}_R(M_3, N) \to \mathbf{Hom}_R(M_2, N) \to \mathbf{Hom}_R(M_1, N) \to \mathbf{Ext}_R(M_3, N) \to 0.$$

Remark 9.11. **Ext** is related to extensions of a R-modules. Given any R-modules M, N, $\mathbf{Ext}_R^1(M, N)$ is isomorphic set of "extensions" $0 \to N \to X \to M \to 0$ of R-modules up to isomorphism. Two extensions are isomorphic if there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & x_1 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\cong} & & \downarrow{\cong} & & \downarrow{\cong} & & \\ 0 & \longrightarrow & N & \longrightarrow & x_2 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Higher **Ext** groups, do something related to classifying exact sequence.

$$0 \to N \to X_y \to \cdots \to X_2 \to X_1 \to M \to 0$$

Theorem 9.12. For a commutative ring R, $\mathbf{Tor}_i^R(M, N)$ can be computed using instead projective resolutions of N, in fact flat resolutions of N, that is,

$$\cdots \to F_1 \to F_0 \to N \to 0$$

is exact with F_i flat.

$\mathbf{Tor}^R(M, N)$ are the homology of the complex

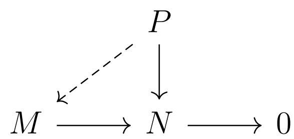
$$\cdots \to M \otimes_R F_1 \to M \otimes_R F_0 \to 0$$

Corollary 9.13.

1. $\mathbf{Tor}_i^R(M, N) \cong \mathbf{Tor}_i^R(N, M)$ uses $M \otimes_R N = N \otimes M$.
2. Could use flat resolution of M as well get long exact sequence too.

Lemma 9.14. Free modules and projective modules are flat.

Proof. Suppose F is free, so $F \cong R^I$ for some I. Consider $0 \to L \to M \to N \to 0$. Then $L \otimes_R F \to M \otimes F \to N \otimes F \to 0$ is isomorphic to $0 \to L^I \to M^I \to N^I \to 0$, since the tensor product commutes with the coproducts and that $N \otimes_R R \cong N$. Now, suppose P is projective, being projective means that in the diagram



with bottom row exact, the map $P \to N$ has a factorization through M. If we take $N = P$ and M as a free module, we can see that P is therefore a retraction of a free module. Therefore, we conclude that projectives are summands of free modules. The converse is true as well.

Therefore, $P \to F \to P$ is the identity, so $- \otimes F \cong (- \otimes P) \oplus (- \otimes P')$ and tensoring with P is exact. □

Given a short exact sequence $L \to M \to N \to 0$, we have a right exact sequence $L \otimes X \to M \otimes X \to N \otimes X \to 0$. We would like to continue the sequence to the left, i.e. exactness at $L \otimes X$. Therefore, we want a functor $\mathbf{Tor}_i^R(-, X)$ so that we have a long exact sequence

$$\cdots \longrightarrow \mathbf{Tor}_1^R(L, X) \longrightarrow \mathbf{Tor}_1^R(M, X) \longrightarrow L \otimes X \longrightarrow M \otimes X \longrightarrow N \otimes X \longrightarrow 0$$

If X is flat we could make this exact sequence just by declaring that all the higher Tors are zero, so we declare that this is so.

We want to compute $\mathbf{Tor}_1^R(N, X)$, we can choose generators for N to get an exact sequence $0 \to K \to R^n \to N \to 0$. Using the long exact sequence, we see $\mathbf{Tor}_1^R(N, X) = \ker(R^{\oplus} \otimes X \to K \otimes X)$ and for $i > 1$ that $\mathbf{Tor}_i^R(N, X) = \mathbf{Tor}_{i-1}^R(K, X)$.

Lemma 9.15. Suppose that $0 \to I \to R \to R/I \to 0$ is an exact sequence and that $0 \to I \otimes_R X \to X \otimes X/2X \to 0$ is exact. Then $\mathbf{Tor}_1^R(R/I, X) = 0$.

Proof. Take the long exact sequence. □

Theorem 9.16. Let X be an R-module. The following are equivalent:

1. X is flat.

2. For any R-modules $N' \subseteq N$ and exact sequence $0 \to N' \to N$, the map $N' \otimes_R X \to N \otimes_R X$ is injective.

3. For any finitely-generated R-modules $N' \subseteq N$, the map $N' \otimes_R X \to N \otimes_R X$ is injective.

4. For any ideal $I \subseteq R$, the map $I \otimes_R X \to R \otimes RX$ is injective.

5. For any finitely-generated ideal $I \subseteq R$, the map $I \otimes_R X \to X$ is injective.

Proof. We have (1) $\iff$ (2), (2) $\Rightarrow$ (3), (2) $\Rightarrow$ (4), (2) $\Rightarrow$ (5), (3) $\Rightarrow$ (5) and (4) $\Rightarrow$ (5).

We need to show (3) implies (2) and (5) implies (4), which were proved in the lemma above. If something is in the kernel of the map $N' \otimes_R X \to N \otimes_R X$, we can check it is zero by looking at finitely-generated submodules.

We can also show that (4) $\Rightarrow$ (3). Note that N is finitely-generated, and therefore $N_0 = N' \subseteq N_1 \subseteq \cdots \subseteq N_k = N$ where $N_i/N_{i-1} \cong R/I_i$. We can assume that for some $j \leq k$, we have $N_j = N_k$. The map $N' \otimes_R X \to N \otimes_R X$ is injective if and only if for every i we have $N_i \otimes_R X \to N_{i+1} \otimes_R X$ is injective.

Let us consider the exact sequence $N_{i-1} \to N_i \to R/I$ and part of the Tor exact sequence $\mathbf{Tor}_1^R(R/I, X) \to N_{i-1} \otimes X \to N_i \otimes X \to R/I \otimes X \to 0$, so since $\mathbf{Tor}_1^R(R/I, X) = 0$, we have that $N_{i-1} \otimes X \to N_i \otimes_X$ injective and X is flat. □

Proposition 9.17. An R-module M is flat if and only if for all finitely-generated ideals I of R, we have that $\mathbf{Tor}_1^R(R/I, M) = 0$.

Proposition 9.18 (The equational criterion for flatness)**.** An R-module X is flat if and only if for every relation $\sum_{i=1}^n r_i x_i$ with $r_i \in R$ and $x_i \in X$, there exists $y_1, \cdots, y_k \in X$ and $a_{ij} \in R$ with $x_i = \sum_{j=1}^r a_{ij} y_j$ for all i and for all j, we have $\sum_{i=1}^n r_i a_{ij} = 0$.

Proof. Suppose that X is flat and that $\sum_{i=1}^n r_i x_i = 0$. Consider the ideal $I = (r_1, \cdots, r_n)$ and the map $0 \to K \to R^n \to I \to 0$. Consider also the exact sequence $0 \to I \to R \to R/I \to 0$. Then we have $\sum_[i = 1]^n r_i \otimes y_i$ is in the kernel of $I \otimes_R X \to R \otimes_R X$. But this tells us there is some $k \in K \otimes_R X$ with k hitting $\sum_{i=1}^n e_i \otimes x_i$, we can write k as $k = \sum_j k_j \otimes y_j$ and $k_j = \sum_{i=1}^n a_{ij} e_i$.

For the other direction, let I be a finitely-generated ideal and suppose that $\sum_{i=1}^n r_i \otimes x_i$ is in the kernel of $I \otimes_R X \to R \otimes_R X$. We want to show that the kernel is trivial. As $\sum_{i=1}^n r_i x_i = 0$ in M, we have

$$x = \sum_{i=1}^n r_i \otimes x_i = \sum_{i=1}^n (r_i \otimes (\sum_{j=1}^k a_{ij} y_j)) = \sum_{j=1}^k \sum_{i=1}^n f_i a_{ij} \otimes y_j = 0.$$

□

We can therefore conclude that $\mathbb{Q}$ is flat as a $\mathbb{Z}$-module.

If A is any torsion group and D is any divisible group, then $A \otimes_{\mathbb{Z}} D = 0$. The argument just needs every element of D to have finite order, so we can in fact see that $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$, and therefore $\mathbb{Q}/\mathbb{Z}$ is not flat.

Corollary 9.19. A R-module X is flat if and only if for any map $f : R^n \to X$ and $x \in \ker(f)$, there is a commuting diagram

$$\begin{array}{ccc} R^n & \xrightarrow{f} & M \\ {\scriptstyle h}\downarrow & \nearrow & \\ R^k & & \end{array}$$

with $x \in \ker(h)$.

Proof. This is just the equational criteria for flatness. An element $x \in \ker(f)$ gives a relation $\sum_{i=1}^{n} r_i x_i = 0$. The $y_1, \cdots, y_k$ gives us a map $R^k \to X$. The map $h : R^n \to R^k$ is given by the matrix $A = (a_{ij})$, where $x_i = \sum_{i=1}^{k} a_{ij} y_j$. This equation tells us that the diagram commutes. □

By the universal property of $\otimes_R$, $\mathbf{Hom}_R(A \otimes_R B, C) \cong \mathbf{Hom}_R(A, \mathbf{Hom}_R(B, C))$ gives the tensor-hom adjunction.

Here $- \otimes_R B$ is the functor within the category of R-modules, and the hom functor $\mathbf{Hom}_R(B, -)$ is the usual hom functor.

Recall that left adjoints preserve all colimits in the domain category, and the right adjoints preserve all limits.

Example 9.20. $- \otimes_R B$ preserves all direct sums, direct limits, and right exact sequences.

A fact is that homology commutes with direct limits of chain complexes. Therefore, we now know that **Tor** commutes with direct limits in each variable.

10 Integral Extensions

Definition 10.1. Let $A \subseteq B$ be a subring, we say $x \in B$ is integral over A if it satisfies a monic polynomial with coefficients in A, i.e. $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for $a_i \in A$.

Example 10.2. For a number field K, i.e. a finite extension of $\mathbb{Q}$, the set of elements in K integral over $\mathbb{Z}$ is called the ring of algebraic integers $\mathcal{O}_K \subseteq K$.

In particular, for $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$.

Lemma 10.3. The following are equivalent.

1. $x \in B$ is integral over A.
2. The A-subalgebra C of B generated by x is finite over A, i.e. finitely-generated as A-module.
3. The A-subalgebra C of B generated by x is contained in some finite A-algebra $D \subseteq B$.
4. There is a faithful C-module M which is finitely-generated as an A-module.

Proof. Note that (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are obvious.

(3) $\Rightarrow$ (2) is true as we view D as a C-module. It is faithful because $1 \in D$.

(1) $\Rightarrow$ (4): Given C, M as above, M is finitely generated by $m_1, \cdots, m_n$ as an A-module. We can choose $a_{ij} \in A$ with $1 \leq i, j \leq n$ such that $xm_i = \sum_{j=1}^{n} a_{ij}m_j \in M$. Then the matrix $Y = (y_{ij})$ with coefficients in C given by $Y = x \cdot I - (a_{ij})$ satisfies

$$Y \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \in M^{\oplus n}$$

For a matrix Y over any commutative ring, the adjugate matrix $\mathbf{adj}(A)$ satisfies $\mathbf{adj}(Y) \cdot Y = Y(\mathbf{adj}(Y)) = \det(Y)$. We multiply equation above by $\mathbf{adj}(Y)$, then we see $\det(Y) \in C$ satisfies $\det(Y) \cdot m = 0$, so $\det(Y)$ annihilates M and so $\det(Y) = 0$, otherwise M is not faithful. But $\det(Y)$ is a monic polynomial in X with coefficients over A, so $x \in B$ is integral over A. $\square$

This lemma will imply if $x, y \in B$ integral over A, then $-x, x+y, xy$ are also integral over A. Hence, the set of elements in B integral over A is called the integral closure of A in B, which is a subring of B containing A.

Lemma 10.4. Let $A \subseteq B$ be a subring. Then the integral closure C of A in B is a subring.

Proof. Clearly $A \subseteq C$ and $0, 1 \in C$. Consider A-submodule D generated by x and y. We claim that D is finite over A. This is true because D is generated by $x^i y^j$ for $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$ for monic polynomials of degree m and n, respectively. Therefore, since $-x, x+y, xy \in D$, the lemma above gives that they are all in C. $\square$

Corollary 10.5. The integral closure of C in B is C, i.e. integral closures are integrally closed.

Proof. Suppose $x \in B$ is integral over C, then x satisfies some monic polynomial. Therefore, x is integral over A-subalgebra generated by $c_0, \cdots, c_{n-1}$ and each c_i is finitely-generated, so x is contained in an A-subalgebra finite over A. Hence, $x \in C$. □

Remark 10.6. An integral algebra of finite type is a finite algebra.

Corollary 10.7. For rings $A \subseteq B \subseteq C$ and suppose B is integral over A and C is integral over B, then C is integral over A.

Corollary 10.8. Let $A \subseteq B$ be rings and let C be the integral closure of A in B, then C is integrally closed in B.

Remark 10.9. Localization preserves the integral property.

Definition 10.10. A domain R is normal if it is integrally closed in the field of fractions of R.

Example 10.11. For any number field K, $\mathcal{O}_K$ is normal.

Example 10.12. A UFD is normal. Therefore, $\mathbb{Z}$ and polynomial rings over K are normal.

Remark 10.13. In geometric terms, an algebraic variety X is normal if every finite birational morphism

$$Y \to X$$

is an isomorphism for variety Y. There is a corresponding map from the regular functions $\mathcal{O}(X)$ to regular functions $\mathcal{O}(Y)$. There is an isomorphism between their fractional fields.

Remark 10.14. Suppose $f : R \to S$ is a map of rings. Then $\otimes_R S$ as map from R-modules to S-modules is left adjoint to f^*, the map from S-modules to R-modules.

Proof. For an R-module A and an S-module B, we have $\mathbf{Hom}_S(A \otimes_R S, B) \cong \mathbf{Hom}_R(A, f^*B)$. □

Suppose R is a ring and M is flat, then $M \otimes_R S$ is flat.

Definition 10.15. A number is algebraic over $\mathbb{Q}$ if it satisfies a polynomial with coefficients in $\mathbb{Q}$. Since Q is a field, we we can make this polynomial monic.

Any power of a can be written in terms of lower power of a and its inverse can be written as a $\mathbb{Q}$-linear combination of powers of a.

Note that we have $\mathbb{Q}(a) = \mathbb{Q}[a]$.

Definition 10.16. Suppose $R \subseteq S$ is an inclusion of rings, and $x \in S$ is integral over R is x satisfies a monic polynomial with coefficients in R.

Definition 10.17. We say $R \subseteq S$ is an integral extension if every element of S is integral over R.

Note that field extensions are integral.

Proposition 10.18. Suppose we have rings $R \subseteq S$ and $x \in S$. The following are equivalent:

1. $x \in S$ is integral over R.
2. $R[x]$ is finitely-generated R-module.
3. $R[x]$ is contained in a subring T of S that is finitely-generated as an R-module.
4. There is a faithful $R[x]$-module M (annihilator of M is 0) that is finitely-generated as an R-module.

Definition 10.19. $R \to S$ is finite if S is finitely-generated as an R-module.

$R \to S$ is finite type if S is finitely-generated as an R-algebra.

Corollary 10.20. Suppose $x_1, \cdots, x_n$ are elements of S and $R \subseteq S$. Suppose $x_1, \cdots, x_n$ are integral over R, then $R \to R[x_1, \cdots, x_n]$ is finite.

Proof. By induction on n. □

Corollary 10.21. Let $R \to S$ be an extension, then the set of elements that are integral over R form a subring.

Proof. If x, y are integral over R, then any element in $R[x, y]$ is integral over R. □

If the integral closure of R in S is S, then S is integral over R and we say $R \subseteq S$ is an integral extension.

A map $f : R \to S$ is integral if S is integral over $f(R)$.

Corollary 10.22. $f : R \to S$ is finite if and only if it is finite type and integral.

Proof. ($\Rightarrow$): Obvious.

($\Leftarrow$): Suppose $f(R) \subseteq S$ is an integral extension of finite type. Note that x_i's are integral over $f(R)$, and $S \cong f(R)[x_1, \cdots, x_n]$. Therefore, $f(R) \subseteq S$. □

Corollary 10.23. If $R \xrightarrow{f} S \xrightarrow{g} T$ is a composition of ring maps and f and g are integral, so $g \circ f$ is integral.

Corollary 10.24. Consider $R \subseteq S$ and T be the integral closure of R in S. Then T is integrally closed in S.

Proof. Look at $R \to T \to T[x]$ for any $x \in S$ that is integral over T. □

Lemma 10.25. Suppose $R \to S$ is an integral extension. Then if $I \subseteq R$ and $J = I \cap S$, then $R/J \to S/I$ is integral, and $(R\backslash J)^{-1}R \to (S\backslash I)^{-1}S$ is also integral.

Proof. Take $x \in R$, we write $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$.

Consider $x/s \in S^{-1}R$. □

Corollary 10.26. $f : A \to B$ is finite if and only if B if finitely-generated A-module over $f(A)$. f is integral and of finite type if and only if B is finitely-generated A-algebra over $f(A)$. Note that the two terms themselves are also equivalent.

Lemma 10.27. Let C be integral closure of A in B. Let S be a multiplicatively closed subset of A. Then $C[S^{-1}]$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Corollary 10.28. Let A be a domain. Then the following are equivalent:

1. A is normal.
2. A_p is normal for every prime ideal $p \subseteq A$.
3. A_m is normal for maximal ideal $m \subseteq A$.

Proof. Note that all these rings have the same fractional field.

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) follows from the lemma above.

(3) $\Rightarrow$ (1): suppose A_m is normal for $m \subseteq A$. Obviously $A \hookrightarrow C$ where C is the integral closure of A. This is surjective because $A_m \hookrightarrow C_m$ is surjective for $m \subseteq A$. □

Example 10.29. For a number field $\mathcal{O}_K$, $\mathcal{O}_K$ is not a UFD in general. But localization of $\mathcal{O}_K$ at maximal ideals are DVR, therefore, PID, UFD, and normal.

Lemma 10.30. Let $A \subseteq B$ be an integral extensions and let $q \in \mathbf{Spec}(B)$. Denote $p = q \cap A \in \mathbf{Spec}(A)$, then q is maximal if and only if p is maximal.

Proof. By the previous lemma, B/q is integral over A/p. Then we want to show if $A \subseteq B$ are domains, and B is integral over A, then we know B is a field if and only if A is a field.

Suppose A is a field, let $y \in B$ be nonzero, then since B is integral over A, then the element satisfies a monic polynomial in $A[x]$. Choose $n > 0$ be minimal such that $a_0 \neq 0$.

Suppose B is a field, let $x \in A\backslash\{0\}$, then $\frac{1}{x} \in B$, so $\frac{1}{x}$ satisfies a monic polynomial over A. In particular, $x^{-1} \in A$. □

Note that for an integral ring homomorphism $f : A \to B$, $q \in \mathbf{Spec}(B)$, let $p = f^{-1}(q)$ be in the spectral of A, then q is maximal if and only if p is maximal. Therefore, integral morphisms of affine schemes send closed points to closed points.

Definition 10.31. For an affine scheme X with data X and R. We write $\mathcal{O}(X) = R$, the ring of regular functions on X. Morphism of affine schemes correspond to ring homomorphsim in the other direction. That is, $X \to Y$ corresponds to $\mathcal{O}(Y) \to \mathcal{O}(X)$.

Example 10.32. $K \hookrightarrow K[x]$ is not finite, and the spectral map $\mathbf{Spec}(K[x]) \to \mathbf{Spec}(K)$ sends generic points to closed point of R. Similarly this works on $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

Corollary 10.33. If $A \subseteq B$ is an integral extension with $q \subseteq q'$ prime in B such that $q \cap A = q' \cap A$ in the spectral of A, then $q = q'$ in the spectrum of B.

Proof. Let $p = q \cap A = q' \cap A$, since $A \subseteq B$ is integral, then $A_p \subseteq B_p$ is integral. Let $m = pA_p$, the maximal ideal of the local ring A_p, then define $n = q \cdot B_p$, $n' = q'B_p$. Clearly $n \subseteq n'$. Moreover, $n \cap A_p = n' \cap A_p = m$. By the previous lemma, both n and n' are maximal in B_p. Therefore, $n = n'$. By the correspondence theorem, $q = q'$. □

Theorem 10.34. Let $A \subseteq B$ be integral and p be integral in A. Then there is a prime $q \in B$ with $q \cap A = p$. Therefore, the map $\mathbf{Spec}(B) \to \mathbf{Spec}(A)$ is an onto map that sends q to $q \cap A$.

Example 10.35. Consider ring homomorphism $k[t] \to k[t, t^{-1}]$. Therefore is a correspondence between $\mathbf{Spec}(k[t, t^{-1}])$ and $\mathbf{Spec}(k[t])$. But this is not a surjective map since $k[t, t^{-1}]$ is not integral over $k[t]$, but its image is dense.

Proof. Since $A \subseteq B$ is integral, then the localization satisfies $A_p \subseteq B_p$ and is integral. We now have a commutative diagram

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A_p & \hookrightarrow & B_p \end{array}$$

and this is injective because localization is exact. A_p is local so $A_p \neq 0$, and so $B_p \neq 0$. Therefore, there is a maximal ideal n inside B_p whose pullback $m = n \cap A_p$ must be maximal by the lemma. Therefore, $m = pA_p$. The one-to-one correspondence gives prime ideal in B that pulls back to p. □

Corollary 10.36. Suppose that $f : R \to S$ is an integral map, then the induced map on spectra is closed.

Proof. We can reduce to the case that f is an integral extension. We claim that for $V(I) \subseteq$ $\mathbf{Spec}(C)$, we have $f^*(V(I)) = V(f^{-1}I)$. We always have that $f^*(V(I)) \subseteq V(f^{-1}(I))$. For the other inclusion, suppose $p \in V(f^{-1}I)$, then $f^{-1}I \subseteq p$, and we need to find some $q \in$ $\mathbf{Spec}(S)$ such that $q \in V(I)$ and $f^{-1}(q) = p$. Consider the integral extension $R/f^{-1}I \to S/I$, there is a $q \in \mathbf{Spec}(S)$ with $I \subseteq q$ and $f^{-1}(q) = p$. ☐

We can reduce the case of going up to having $p_0 \subseteq p_1 \in \text{Spec}(R)$, and a q_0 in $\mathbf{Spec}(S)$ with $q_0 \cap R = p_0$. We want to find a q_1 containing q_0 and $q_1 \cap R = p_1$. Consider the integral extension $R/p_0 \to S/p_0$. Applying results above, the map gives a prime ideal q_1 containing q_0 and pull back to p_1.

Proposition 10.37. Suppose B is integral over A, then B is a field if and only if A is a field.

Theorem 10.38. Let B/A be an integral extension and let p be a prime ideal of A. Then there exists a prime ideal q of B such that $q \cap A = p$.

Theorem 10.39 (Going-up Theorem)**.** Suppose B/A is integral, and let $p_1 \subseteq \cdots \subseteq p_n$ be a chain of prime ideals of A, and $q_1 \subseteq q_m$ $(m < n)$ be a chain of prime ideals of B such that $q_i \cap A = p_i$, then the chain of q_i's can be extended to a chain $q_1 \subseteq \cdots \subseteq q_n$ such that $q_i \cap A = p_i$ for all i.

Definition 10.40. A ring map $f : R \to S$ has the going up property if for any prime ideals $p_0 \subseteq p_1 \subseteq R$ and $q_0 \subseteq S$ with $f^{-1}q_0 = p_0$, then there is a q_1 containing q_0 such that $f^{-1}q_1 = p_1$.

Remark 10.41. The going up property is equivalent to the following. For any chain of primes $p_0 \subseteq \cdots \subseteq p_n$ in R and chain $q_0 \subseteq q_m$ with $0 \leq m < n$ with $f^{-1}q_i = p_i$ for $0 \leq i \leq m$, it can be extended to a chain of length n with $f^{-1}q_i = p_i$ for all $0 \leq i \leq n$.

Remark 10.42. Going up is stable under composition.

Definition 10.43. For a topological space X, a point $x \in X$ is a specialization of $x' \in X$ and x' is a generalization of x if $x \in \overline{\{x'\}}$.

Therefore, for $x, x' \in \mathbf{Spec}(R)$, we have that x is a specialization of x' if $x \in V(p_{x'})$, i.e. $p_{x'} \subseteq p_x$.

A subset $Y \subseteq X$ is called specialization closed if all specializations of elements of Y are also in Y, i.e. if $y \in Y$, then $\bar{y} \subseteq Y$ as well. Correspondingly, we define the term generalization closed. Therefore, closed subsets are specialization closed and open subsets are generalization closed.

Definition 10.44. A map $f : X \to Y$ is specializing if for any y a specialization of $y' \in Y$ and $x' \in X$ with $f(x') = y'$, there is a specialization x of x' with $f(x) = y$. (If f has the corresponding property for generalizations, the map is generalizing.)

Proposition 10.45. Suppose that $f : X \to Y$ is a closed map of topological spaces. Then f is specializing.

Proof. Suppose that y is a specialization of y' and $f(x') = y'$ where $x' \in X$. Since f is closed, then $f(\overline{x'})$ is closed, and $\overline{y'} \subseteq f(\overline{x'})$. Since $y \in \overline{y'}$, there is some $x \in X$ with $f(x) = y$. □

Proposition 10.46. A map $f : R \to S$ satisfies going up if and only if the induce map $f : \mathbf{Spec}(S) \to \mathbf{Spec}(R)$ is specializing.

Lemma 10.47. Suppose that $f : R \to S$ is a map of rings. Then the image of $\mathbf{Spec}(S)$ in $\mathbf{Spec}(R)$ is specialization closed if and only if the map itself is closed.

Proof. Clearly closed implies specialization closed. Suppose that the image is specialization closed. Replace $R \to S$ by $R/I \hookrightarrow S$, so we can assume that the map f is injective. We claim that the map $\mathbf{Spec}(S) \to \mathbf{Spec}(R)$ hits every minimal prime of R. If $p \in \mathbf{Spec}(R)$ is minimal, consider $R_p \to S_p$. Since p is minimal and so R_p is field. It is enough to show that S_p is not zero, according to the exactness of localization. Therefore, if the image of $\mathbf{Spec}(S)$ in $\mathbf{Spec(R)}$ is specializing, the image contains every minimal prime of $\mathbf{Spec}(R)$, therefore closed. □

Theorem 10.48. Let $f : R \to S$ be a ring map. The following are equivalent:

1. $\mathbf{Spec}(S) \to \mathbf{Spec}(R)$ is closed.
2. f has the going up property.
3. For any $q \in \mathbf{Spec}(S)$ and $f^{-1}(q) = p$ in $\mathbf{Spec}(R)$, the map $\mathbf{Spec}(B/q) \to \mathbf{Spec}(R/p)$ is surjective.

Proof. (2) implies (1): consider $V(I) \subseteq \mathbf{Spec}(S)$. We want to show that the image of $V(I)$ is closed in $\mathbf{Spec}(R)$. Consider $R \xrightarrow{f} S \to S/I$, it is enough to show that the image of $\mathbf{Spec}(S/I) \to \mathbf{Spec}(R)$ is closed. Note that $R \to S/I$ satisfies going up. We only need to show that the image of $\mathbf{Spec}(S/I)$ in $\mathbf{Spec}(R)$ is specialization closed. Since $\mathbf{Spec}(S/I)$ is specialization closed and the map $\mathbf{Spec}(S/I) \to \mathbf{Spec}(R)$ is specialization, so its image is also specialization closed. □

Definition 10.49. A domain is normal or integrally closed if it is integrally closed in its field of fractions. The normalization of a domain is its integral closure in its field of fractions.

Example 10.50. We have seen that $\mathbb{Z}$ is normal. For K is a field, $K[x]$ is normal. UFDs are normal. $\mathbb{Z}[\sqrt{5}]$ is not normal.

Consider $k[x,y]/(y^2-x^3)$, then this is isomorphic to $k[t^2,t^3]$ where $y\mapsto t^3$ and $x\mapsto t^2$. The field of fractions is $k(t)=k[t]$ since t is integral over $k[t^2,t^3]$, we see that the normalization of $k[x,y]/(y^2-x^3)$ is $k[\frac{y}{x}]$.

This corresponds to $\mathbb{A}^1_k \to \mathbf{Spec}(K[t^2,t^3])$ and resolve the cusp.

Proposition 10.51. For $R\subseteq S$ set T be the integral closure of R in S. Then for any multiplicatively closed subset M of S, we have that $M^{-1}T$ is in the integral closure of $M^{-1}R$ in $M^{-1}S$.

Proof. We have $M^{-1R}\to M^{-1}T$ is integral. If $\frac{s}{m}\in M^{-1}S$ is integral over $M^{-1}R$, consider the equation $(\frac{s}{m})^k+\frac{r_1}{m_1}(\frac{s}{m})^{k-1}+\cdots+\frac{r_k}{s_k}=0$. Multiply by $(mm_1\cdots m_k)^k$ to get that $sm_1\cdots m_k$ is integral over R. This implies $sm_1\cdots m_k\in T$ and $\frac{s}{m}\in M^{-1}T$. □

Proposition 10.52. Let R be an integral domain. Then the following are equivalent.

1. R is normal.
2. A_p is normal for all $p\in\mathbf{Spec}(R)$.
3. A_m is normal for all maximal ideal m.

Proof. Let S be the normalization of R in $R_{(0)}$. Moreover, note that the field of fractions of any of the localizations of R is just $R_{(0)}$ again. So we are trying to show that $R\to S$ is a surjective. By the previous theorem, we have that S_p is the normalization of R_p for every p. So we can use the fact that a map of rings is surjective if and only if it is locally surjective. □

Lemma 10.53. Let T be the integral closure of R in S and let I be an ideal in R and $J=IT$. Then the set of all elements of S satisfying an monic polynomial with coefficients in I is $\sqrt{J}$. We call this property of satisfying a monic polynomial with coefficients in I as being integral over I.

Proof. If $x^n+j_1x^{n-1}+\cdots+j_n=0$ with the j_i's in I, we see that $x^n\in J$, so $x\in\sqrt{J}$. For the other direction, if $x^n=\sum_{i=1}^k j_ix_i$ for $j_i\in I$ and $x_i\in T$, we see that $x^n\in R[x_1,\cdots,x_k]$, which is a finitely-generated R-module and we see that $x^nR[x_1,\cdots,x_n]\subseteq IR[x_1,\cdots,x_n]$. By Cayley-Hamilton theorem, x^n satisfies a monic polynomial with coefficients in I, so x does as well. □

Recall that $K \subseteq L$ an extension of fields, we say that $l \in L$ is algebraic over K is it is integral over K. Any such algebraic element satisfies a unique minimal polynomial, that is a monic polynomial of minimal degree.

Proposition 10.54. Suppose that $R \subseteq S$ are domains with R normal and suppose that $x \in S$ integral over $I \subseteq R$. Then x is algebraic over the fractional field of R, and the minimal polynomial over K has all coefficients in $\sqrt{I}$.

Proof. Since x is algebraic over K, the fractional field of R is immediate. For the other claim, consider some extension of L that has all the roots of the minimal polynomial of x, i.e. the minimal polynomial of x splits in L as $\prod_{i=1}^{n}(t - x_i)$. Each of the x_i's is integral over I, since the coefficients of the minimal polynomial of x are polynomials in x_i's. We see that these are all integral over I, so the coefficients in $\sqrt{I}$. □

Lemma 10.55. If $R \to S$ is an inclusion of rings then $p \in \mathbf{Spec}(R)$ is in the image of $\mathbf{Spec}(S)$ if and only if $R \cap pS = p$.

Proof. ($\Rightarrow$): Obvious.

($\Leftarrow$): Suppose $R \cap pS = p$ and let $T = R \backslash p$ in S, then pS does not intersect T, so looking at $R_p \to S_p$, we know pS_p is contained in some maximal ideal of S_p. Taking the pullback of this map, we get back to a prime in S, and it contains pS and it does not intersect with T. This pulls back p. □

Theorem 10.56 (Going Down)**.** Let $R \subseteq S$ be an integral extension of domains where R is normal. The map $\mathbf{Spec}(S) \to \mathbf{Spec}(R)$ is generalizing, in other words if there is $p_0 \in \mathbf{Spec}(R)$ of the form $q_0 \cap R$ and p_0 is a generalization of p_1, i.e. $p_0 \in \bar{p}_1$, or $p_0 \supseteq p_1$, then there exists a $q_1 \in \mathbf{Spec}(S)$ with $q_1 \cap R = p_1$.

Proof. Consider the diagram

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ R_{p_0} & \longrightarrow & S_{q_0} \end{array}$$

we need to show that p_1 is the pullback of a prime in S_q. It is enough to show that the pullback of $p_1 S_{q_0}$ to R is p_1. Every $x \in p_1 S_{q_0}$ is of the form $\frac{y}{t}$, where $y \in p_1 S$ and $t \notin q$. This y must be integral over p_1 by the lemmas above. Therefore, we know that the minimal polynomial of y must have the form $y^r + u_1 y_{r-1} + \cdots + u_n$ with u_i's in p_1. Therefore, for $x \in R \cap p_1 S_{q_0}$, we have that $t = \frac{y}{x}$ and the minimal polynomial for t over K is obtained by dividing the above minimal polynomial by x^n, we get that $t^n + v_1 t^{r-1} + \cdots + r_n = 0$, where $v_i = \frac{u_i}{x_i}$. We see that $x^i v_i \in p_1$. Since t is integral over R, each v_i is in R by the previous lemma. If $x \notin p_1$, then each $v_i \in p_1$, so $t^n \in p_1 R \subseteq p_0 R \subseteq q_0$ and $t \in q_0$. This is a contradiction. □

11 Valuation Ring

Definition 11.1. For R an integral domain with field of fractions K, we say that R is a valuation ring of K if for each nonzero $x \in K$, either x or x^{-1} are in R.

Example 11.2. Any field is a valuation ring. More interestingly, $\mathbb{Z}_{(p)}$ is a valuation ring.

Proposition 11.3. Let R be a valuation ring of K. Then

1. R is a local ring.
2. If $R \subseteq R' \subseteq K$, then R' is a valuation ring.
3. R is normal.

Proof. 1. Let m be the set of non-units in R, so for $x \in m$ either $x = 0$ or $x^{-1} \in R$. For $r \in R$ and $x \in m$, we have $rx \in m$, otherwise $(rx)^{-1} \in R$ and $r(rx)^{-1} = x^{-1} \in R$. For x, y nonzero elements of m, either xy^{-1} or $x^{-1}y$ is in R. Without loss of generality, suppose that $xy^{-1} \in R$. Then $(1 + xy^{-1})y \in m$, so $x + y \in m$. We conclude that m is an ideal, so R is therefore local.

2. By definition.

3. Suppose that $x \in K$ is integral over R, so $x^n + r_1 x^{n-1} + \cdots + r_n = 0$. If $x \in R$, then we are done. If not, then $x^{-1} \in R$. Divide the equation by x^{n-1}, then $x \in R$.

□

Remark 11.4 (Construction)**.** For K a field and Ω algebraically closed field, let Σ be the set of all pairs (R, f) where R is a subring of K, and $f : R \to \Omega$ is a ring homomorphism. Put a partial order on Σ by inclusion and that the maps are compatible. Using Zorn's lemma, we know there is a maximal element S of Σ. We want to show that S with $g : S \to \Omega$ is a valuation ring.

Lemma 11.5. S is local with maximal ideal $m = \ker(g)$.

Proof. Clearly $\ker(g)$ is prime. Extend g to a map $S_m \to \Omega$ by sending $\frac{s}{t} \mapsto \frac{g(s)}{g(t)}$. By maximality, it follows that $S_m = S$, and so S is local. □

Lemma 11.6. For $0 \neq x \in K$, let $m[x] = mS[x]$, then either $m[x] \neq S[x]$ or $m[x^{-1}] \neq S[x^{-1}]$.

Proof. Suppose the two equalities hold. Then we have that $u_0 + u_1x + \cdots + u_mx^m = 1$, and $v_0 + v_1x^{-1} + \cdots + v_nx^{-n} = 1$. Without loss of generality, suppose that m and n are as small as possible. Suppose $m \geq n$ and multiply the equation by x^n. This gives $(1-v_0)x^n = v_1x^{n-1} + \cdots + v_n$. Since $v_0 \in m$, we conclude that $1-v_0$ is a unit. Therefore, we can write this equation as $x^n = w_1x^{n-1} + \cdots + w_n$ with $w_i \in m$. Therefore, we can rewrite the first equation using terms of lower degrees. This gives a contradiction. □

Theorem 11.7. S is a valuation ring of K.

Proof. Given a nonzero $x \in K$, we need to show that either $x \in S$ or $s^{-1} \in S$. Assume $m[x]$ is not all of $S[x] = s'$, then it must be contained in a maximal ideal m', and $s \cap m' = m$. Therefore, $K = S/m \hookrightarrow S'/m' = K'$. Note that $K' = K[x]$, and it is a field. Therefore, x is algebraic over K, and K' is a finite extension of x. There is an embedding of R/m into Ω. Therefore, we can extend this into an embedding of K' into Ω, since Ω is algebraically closed. Then we can get a map $S' \to \Omega$ extending that $S \to \Omega$, so we have $S = S'$ and $x \in S$. □

Corollary 11.8. For R a domain the normalization of $R = \bar{R}$ is the intersection of all valuation rings of K that contain R.

Proof. Any valuation ring contains the normalization since the valuation rings are integrally closed. Take some $x \notin \bar{R}$, then $\bar{x} \notin R[x^{-1}]$ otherwise x would be integral over R, so x^{-1} is not a unit in $R[x^{-1}]$, and is therefore contained in some maximal ideal m'. Take Ω to be the algebraic closure of $R[x^{-1}]/,'$, the restricting R to $R[x^{-1}] \to R[x^{-1}]/m' \to \Omega$ gives a nonzero homomorphism of R into Ω. We can extend this to some valuation ring S containing R and $R[x^{-1}]$ since x^{-1} maps to zero in Ω, so x is not contained in S. □

Lemma 11.9. Let R be a field and let f be a nonzero element of $R[x_1, \cdots, x_n]$, then there is an isomorphism $k[x_1, \cdots, x_n] \xrightarrow{\cong} k[y_1, \cdots, y_n]$ of k-algebras that f becomes a nonzero constant times a monic polynomial in $y_1, \cdots, y_n$. That is, for some $d \geq 0$, $f = cy_n^d + \sum_{i=0}^{d-1} f(y_1, \cdots, y_{n-1})$.

Remark 11.10. Geometrically, given an hypersurface $\{f = 0\} \subseteq \mathbb{A}_k^n$ and we can change coordinates so that the projection $\mathbb{A}_k^n \to \mathbb{A}_k^{n-1}$ given by $(y_1, \cdots, y_n) \mapsto (y_1, \cdots, y_{n-1})$ becomes a finite morphism.

Example 11.11. Let $f = x_1x_2 - 1$, then we have a morphism between affine spaces $k[x] \to k[x_1, x_2]/(x_1x_2 - 1)$ sending $\{f = 0\} \subseteq \mathbb{A}^2 \to \mathbb{A}^1$ from (x_1, x_2) to x_1. This is not finite, but the lemma tells us we can change the coordinates by taking $x_1 = y_1 + y_2$ and $x_2 = y_1 - y_2$. f then becomes $y_1 - y_2^2 - 1$.

Lemma 11.12 (Noether Normalization Lemma)**.** Let R be a nonzero finitely-generated algebra over k. Then there is a natural number n and inclusion $k[x_1, \cdots, x_n] \hookrightarrow R$ such that R is finite over $k[x_1, \cdots, x_n]$.

Proof. There is a surjection $k[x_1, \cdots, x_N] \twoheadrightarrow R$. Suppose N is minimal with this property, we can prove by induction on N.

The base case is when $N = 0$, then we have $k \twoheadrightarrow R$, so either $R = 0$ or $R = k$, either case the ring is finite over the polynomial ring.

To prove the inductive step. Let $I = \ker(k[x_1, \cdots, x_n]) \twoheadrightarrow R)$. If $I = 0$, then we are done. Otherwise, we pick nonzero element f of I. By the previous lemma, we change the coordinates of our N generators, can assume $f = c(x_N^d + \sum_{i=1}^{d-1} a_i(x_1, \cdots, x_{N-1})x_N^i$ for $c \neq 0$. Note $d > 0$ or else f is a unit.

Remove c, the elements are still in I. It follows that R is finite over subalgebra $S = \mathbf{Im}(k[x_1, \cdots, x_{N-1}]) \subseteq R$. By induction, S is finite over a polynomial ring $k[x_1, \cdots, x_n] \subseteq S$. Therefore, R is also finite over $k[x_1, \cdots, x_n]$. □

Remark 11.13 (Geometric Translation)**.** If X is a nonempty affine scheme of finite type over k, there is an n and a finite morphism of affine schemes $X \to \mathbb{A}_k^n$ that is surjective.

We already showed that $k[x_1, \cdots, x_n] \hookrightarrow R$ is finite, and with a corresponding map $\mathbf{Spec}(R) \twoheadrightarrow \mathbf{Spec}(k[x_1, \cdots, x_n]) = \mathbb{A}_R^n$.

An affine scheme over a commutative ring A means an affine scheme X with a map $\mathbf{Spec}(B) = X \to \mathbf{Spec}(A)$, which corresponds to a ring homomorphism $A \to B$.

Corollary 11.14 (Weak Hilbert's Nullstellensatz)**.** Let R be an algebra of finite type over K. If R is a field and R is finite over K (so R has finite dimension as a K-vector space).

Proof. By Noether Normalization Lemma, there is an inclusion $K[x_1, \cdots, x_n] \hookrightarrow R$ with R finite over $K[x_1, \cdots, x_n]$ since R is a field. Note $(0) \subseteq R$ is a maximal ideal so its preimage is maximal, so $K \hookrightarrow R$, and therefore R is a finite k-algebra. □

Corollary 11.15. If K is an algebraically closed field, and any maximal ideal in $K[x_1, \cdots, x_n]$ is of the form $(x_1 - c_1, \cdots, x_n - c_n)$ for some $c_1, \cdots, c_n \in K$. Therefore, the set of all closed points are K^n.

Proof. Take $m \subseteq k[x_1, \cdots, x_n]$ maximal. Then $k[x_1, \cdots, x_n]/m$ is a field, which is a k-algebra of finite type, hence finite over k. Thus, $k[x_1, \cdots, x_n]/m = k$. Therefore, $x_i \mapsto c_i \in R$ gives the map $k[x_1, \cdots, x_n] \to k[x_1, \cdots, x_n]/m = k$. We then have $m = (x_1 - c_1, \cdots, x_n - c_n)$. □

Remark 11.16. This corollary is not true for fields in general. For example, $k^n \hookrightarrow \mathbb{A}_k^n$ mapping to closed points, but there are other closed points, e.g. $(x^2+1) \in \mathbb{R}[x]$.

Definition 11.17 (Jacobson Radical)**.** The Jacobson radical of a commutative ring R is the intersection of all maximal ideals in R. We showed that intersection of all prime ideals in R is nilradical. In general, Jacobson radical may be bigger, e.g. in most local rings.

Example 11.18. Let $R = \mathbb{Z}_{(2)}$ is a domain, so the nilradical ideal is 0. But (2) is the only maximal ideal.

Lemma 11.19. Let R be an algebra of finite type over a field K. Then the Jacobson radical of R is the nilradical of R.

Proof. Clearly, the nilradical is contained in the Jacobson radical. Suppose f is in the Jacobson radical R. We want to show f belongs to every prime p. If we replace R by R/p, which is still algebra of finite type over a domain. Clearly f is contained in the nilradical ideal of the new R as it is still a domain. Suppose $f \neq 0$, $R[\frac{1}{f}] =\subseteq \mathbf{Frac}(R)$ is still of finite type. Now $R[\frac{1}{f}] \neq 0$ because it contains a maximal ideal.

By the weak Nullstellensatz, $R[\frac{1}{f}]/m$ is a field that is finite over K. Let n be the kernel of $R \to R[\frac{1}{f}] \to R[\frac{1}{f}]/m$, denoted g. The image of g is a domain, hence a field. Therefore, n is maximal with $f \notin n$, contradiction, so $f = 0$. □

Definition 11.20. Let R be a commutative ring. The codimension of $I \subseteq R$ is the supremum of length of all chains of primes contained in I: $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq I$. Geometrically, this is counting chains of irreducible closed subsets starting at $V(p)$.

Lemma 11.21. The codimension of p is the dimension of R_p.

Example 11.22. If R is a domain, (0) is a prime ideal of codimension 0. In this case, $R_{(0)}$ is a field. Therefore, the dimension of $R_{(0)} = 0$.

If R is Noetherian normal domain and $p \subseteq R$ is a codimension 1 prime ideal, then $\dim(R_p) = 1$, so R_p is a DVR.

Example 11.23. Let R be a UFD and f be an irreducible element, then (f) has codimension 1, i.e. ($0 \subsetneq (f)$ is maximal chain) and $R_{(f)}$ is a DVR.

This induces the discrete valuation.

Recall for a local Noether domain R of dimension 1, R is a DVR if and only if R is normal if and only if $\dim(m/m^2) = 1$. This structure m/m^2 is called the Zariski cotangent space of $\mathbf{Spec}(R)$ at m.

Example 11.24. Denote $R = K[x_1, \cdots, x_n]$, $m = (x_1, \cdots, x_n)$. Then m/m^2 is a K-vector space with basis $x_1, \cdots, x_n \cong K^n$. This is a cotangent space because elements of R are like functions, we modulo out by those that vanish in order 2.

Consider $R = \mathbb{C}[x, y]/(x^2 - y^3)$. Then $m = (x, y)$. Now $\dim(m/m^2) = 1$ for ring not normal. One can check that $m/m^2 = (x, y)/(x^2, xy, y^2) \cong K^2$.

Remark 11.25 (Dimension of a Polynomial Ring)**.** We want to show that for a field K and $n \geq 0$, $\dim(K[x_1, \cdots, x_n]) = n$. Consider a finite extension $K[x_1, \cdots, x_n] \subseteq R$, we showed that $\mathbf{Spec}(R) \to \mathbf{Spec}(K[x_1, \cdots, x_n])$ is finite and surjective. If we know $\dim(\mathbb{A}_k^n) = n$, then $\dim(R) \geq n$.

We now prove this statement. Look at chain of $p_i = (x_1, \cdots, x_i) \subseteq K[x_1, \cdots, x_n]$, lift these to R using surjection. First lift $p.$ to $q.$ in R. Then $A/p_0 \subseteq R/q_0$ and this inclusion is finite. Therefore, we get prime R/q_0, q_1/q_0 mapping to p_1/p_0, and we can continue getting a chain of n ideals in R. If we have $\dim(R) = n$, then suppose there is a longer chain, then the inclusions remain strict in $K[x_1, \cdots, x_n]$ by a previous lemma. Therefore, the chain has length at most n.

Theorem 11.26. For a field K and $n \geq 0$, $\dim(K[x_1, \cdots, x_n]) = n$.

Proof. We use induction on n. We already know that $\dim(K[x_1, \cdots, x_n]) \geq 0$ and $\dim(K) = 0$, and $\dim(K[x]) = 1$.

Consider $P_0 \subsetneq \cdots \subsetneq P_r$ of length r in $K[x_1, \cdots, x_n]$ with $r \leq n$. Here $P_1 \neq 0$, so we can pick $f \neq 0$ in P_1. By the previous lemma, we can change variable so that f has highest order term to be ax_n^d for some $a \in K$, $a \neq 0$. Then $K[x_1, \cdots, x_n]/(f)$ is free on $\{1, x_n, \cdots, x_n^{d-1}\}$ as a module over $K[x_1, \cdots, x_{n-1}]$. So $K[x_1, \cdots, x_n]/P_1$ is finite over $K[x_1, \cdots, x_{n-1}]$. By the proof of Noether normalization, we know $K[x_1, \cdots, x_n]/P_1$ is finite over some subring of $K[x_1, \cdots, x_s]$ for $s \leq n-1$ so $\dim(K[x_1, \cdots, x_n]/P_1) = s \leq n-1$. By induction, we know $\dim(K[x_1, \cdots, x_n]) \leq n$. □

Corollary 11.27. For R a domain of finite type over a field K, $\dim(R) = \text{trdeg}(\mathbf{Frac}(R)/K)$.

Definition 11.28. Given $F \subseteq E$ a finite extension and $\mathbf{trdeg}(E/F)$ is $|I|$ where $F \subseteq F(x_i) \subseteq E$ where $i \in I$, and the inclusion in E is algebraic.

Note that this is well-defined, as we can see by expressing R as finite extension of $K[x_1, \cdots, x_n]$ and then take the fraction field.

Proposition 11.29. Let R be a UFD and f be irreducible in R. Then (f) is a codimension-1 prime ideal.

Proof. (f) is always prime for f irreducible in a UFD, and $\mathbf{codim}(f) \geq 1$ since $(0) \subsetneq (f)$ has codimension 1. If not, get $(0) \subsetneq q \subsetneq (f)$ where $f \notin q$. For $g \in q$, $g = fh$ for some $h \in R$ since q is prime, so $h \in q$, then $q = fq = f^2q = f^3q = \cdots$. Therefore, if $g \in q$ is a multiple of f^r for any ≥ 0, by the property of UFD, then $g = 0$, so $q = 0$, contradiction. ☐

Theorem 11.30 (Krull's Principal Ideal Theorem)**.** Let R be Noetherian and $x \in R$. Then every minimal prime ideal containing (x) has codimension at most 1.

Geometrically, for $x \in R$, the minimal primes containing (x) corresponds to irreducible components of $\{x = 0\}$. Therefore, the theorem says that all of the components have codimension at most 1.

Remark 11.31. This is not true for polynomial functions in $\mathbb{R}^n$. For example, $\{x^2 + y^2 = 0\} \subseteq \mathbb{R}^2 = \mathbb{A}_{\mathbb{R}^2}$ has codimension 2.

Proof. First reduce via localization. Let P be the minimal prime in R containing (x). We want to show that the codimension of P is at most 1, or equivalently, that $S = R_P$ has dimension at most 1. Here S is local, Noetherian, and $x \in S$, and $m = pR_p \subseteq S$ is a minimal prime ideal containing (x). In fact, this is the only one because m is maximal.

Equivalently, $\sqrt{(x)} = m \subseteq S$. If $q \subsetneq m$ is prime, we need to show the codimension of q is 0. Note that if there is so such q, then we are done. We have $\mathbf{Spec}(S/(x)) = \mathbf{Spec}(S/m)$, $S/(x)$ is Noetherian has dimension 0, and therefore is Artinian. Therefore, the chain of descending ideals in $S/(x)$ terminates: $q(S/x))^{(1)} \supseteq q(S/x)^{(2)} \supseteq \cdots$. Therefore, consider in S, we have $(x) + q^{(1)} \supseteq (x) + q^{(2)} \supseteq \cdots$ terminates. Therefore, for some $n \geq 1$, we have $q^{(n)} + (x) = q^{(n+1)} + (x)$.

We now need to form sequence of symobolic power of q. For a prime ideal q, the nth symbolic power $q^{(n)}$ of q is the inverse image under $S \to S_q$ of q^nS_q. That is, $f \in q^{(n)}$ if and only if f vanishes to order at least n at generic point of $V(q)$.

Recall $\sqrt{(x)} = m$ which is strictly bigger than q, so $x \notin q$, so x maps to a unit in R_q. Thus, for any $f \in q^{(n)}$, $f = ax + g$, $a \in S$, and $g \in g^{(n+1)}$, therefore $ax \in q^{(n)}$, so $ax \in q^nS_q$, where x is a unit. Therefore, $a \in q^nS_q$, i.e. $a \in q^{(n)} \subseteq S$.

Since $x \in m$, this means $q^{(n)}/(q^{(n+1)} + mq^{(n)}) = 0$, i.e. $[q^{(n)}/q^{(n+1)}] \otimes SS/m = 0$. By Nakayama Lemma, $q^{(n)}/q^{(n+1)} = 0$, so $q^{(n)} = q^{(n+1)}$. Any ideal in S_q is generated as an ideal by intersection with S, so we know that $q^nS_q = q^{n+1}S_q$. Taking the tensor product gives $q^nS_q \otimes_{S_q} (S_q/qS_q) = 0$ and $q^nS_q = 0$, according to Nakayama Lemma. The last expression is the condition for a local Noetherian ring to be Artinian. Hence, the dimension and codimension of S_q are both 0, as desired. □

Corollary 11.32. Let R be Noetherian ring with $x_1, \cdots, x_n \in R$. Then every minimal prime ideal containing $(x_1, \cdots, x_n)$ has codimension at most n.

Proof. Do induction. □

Remark 11.33. For any commutative ring R, the dimension of R is the supremum of dimension of R_m for maximal ideals m of R, and this is equivalent to the supremum of codimension of m over all maximal ideals m.

Each $\dim(R_m)$ is finite, but it could happen that $\dim(R) = \infty$.

Example 11.34. There are Noetherian rings of infinite dimension.

Definition 11.35. A commutative ring R is catenary if for any prime ideals $p \subseteq q \subseteq R$, there is a maximal chain $p \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subseteq P_r = q$, and the number r is unique.

Remark 11.36. All algebras of finite type over a field are catenary.

Remark 11.37. There are non-catenary Noetherian local rings due to the example above.

Corollary 11.38. Let R be a domain of finite type over a field. Then for any $p \subseteq R$, we have $\dim(R) = \operatorname{codim}(p) + \dim(R/p)$.

Remark 11.39. Use the fact that for a domain R of finite type over a field K, for any m, $\dim(R) = \dim(R_m)$.

Remark 11.40. The corollary fails if R is not a domain.

Theorem 11.41. Let R be a Noetherian domain. Then R is a UFD if and only if every codimension-1 prime ideal in R is principal.

If R is a UFD, the codimension-1 subvarieties are always defined by a single equation.

Proof. ($\Rightarrow$): Let R be a Noetherian UFD. Let $p \subseteq R$ be a codimension-1 prime ideal. Then $(0) \subsetneq p$ and there is no prime between them. Let $f \in p$ be nonzero, then $f = f_1 \cdots f_r$ with f_i being irreducible. So we know $f_i \in p$ for some i. Suppose we have $f_1 \in p$, then (f_1) is prime by UFD, so $0 \subsetneq (f_1) \subseteq p$, i.e. $p = (f_1)$.

($\Leftarrow$): Suppose R is Noetherian, then every codimension-1 prime is principal. First, show that every nonzero non-unit in R is a product of irreducibles. Suppose this is not the case, then we can choose some f that cannot be written be such a product. Thus, $f = gh$ where g

and h are non-units. Then either g or h is not such a product. By repeating the process, we have a sequence $(f) \subsetneq (g) \subsetneq \cdots$ of strictly increasing principal ideals. We get a contradiction because we see that every nonzero non-unit is a product of irreducibles. This only required R to be a Noetherian domain.

We know every irreducible element f generates a prime. By definition, f is not a unit so $(f) \subsetneq R$. Therefore, there is a minimal prime containing (f). By Krull's principal ideal theorem, p has codimension at most 1, but $(0) \subsetneq (f)$, so it has codimension exactly 1. Then by assumption, p is principal, then $p = (g)$, so $f = gh$. Therefore, h is a unit, and so $(f) = (g) = R$.

Using this, we have a unique factorization. Suppose $f_1 \cdots f_r = g_1 \cdots g_s$ are two irreducible factorizations. Suppose $g_1 \cdots g_s \in (f_1)$, then $g_i \in (f_i)$, and so $g_i = f_1 u$ since f_1 is prime. We cancel the term and proceed by induction. □

Remark 11.42. For any Noetherian normal domain R, we define an Abelian group $\mathbf{Cl}(R)$ as the divisor class group of R generated by codimension-1 prime ideals of R such that $\mathbf{Cl}(R) = 0$ if and only if all codimension-1 prime ideals are principal, if and only if R is a UFD.

$\mathbf{Cl}(R)$ measures failure to be a UFD. A lot of algebraic geometry is concerned with computing this group and closed related to the Picard group.

Lemma 11.43. Let R be a Noetherian local ring and $\mathfrak{m}$ be a maximal ideal. Then $\dim(R) \leq \dim_k(m/m^2)$.

Proof. Since R is Noetherian, $\mathfrak{m}$ is a finitely-generated module, then $\mathfrak{m}/\mathfrak{m}^2$ is a finite-dimensional space and if $e_1, \cdots, e_n$ is a basis, then by Nakayama Lemma, we can lift them to $e_1, \cdots, e_n \in \mathfrak{m}$, and they always generate $\mathfrak{m}$. By corollary to Krull's theorem, $\dim(R) = \operatorname{codim}(\mathfrak{m}) \leq n$. □

Definition 11.44. A Noetherian local ring is regular if $\dim(R) = \dim_k(m/m^2)$.

Example 11.45. A regular local ring R of dimension 0, we have $m/m^2 = 0$, then $m = 0$ by Nakayama Lemma, so R is a field.

Note that $k[x]/(x^{10})$ is dimension 0 but not regular.

Remark 11.46. Every regular local ring is a domain.

Given the remark above, let R be regular local of dimension 1. Then R is Noetherian local domain of dimension 1. Now $\mathfrak{m}/\mathfrak{m}^2$ has dimension 1 and these imply that R is a DVR.

Example 11.47. $K[x_1, \cdots, x_n]_{(x_1,\cdots,x_n)}$ is regular local of dimension n.

Lemma 11.48. For any commutative ring A with a maximal ideal $\mathfrak{m}$, $k = A/\mathfrak{m}$, then $\dim(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}})$.

Proof. We prove the statement $R/\mathfrak{m}^2 \cong R_{\mathfrak{m}}(\mathfrak{m}R_{\mathfrak{m}})^a$. Then $R/\mathfrak{m}^a$ is local. Therefore, its localization at $\mathfrak{m}$ is the same thing: elements of $R\backslash\mathfrak{m}$ are units in $R/\mathfrak{m}^a$ since it is local.

Now consider exact sequence $0 \to \mathfrak{m}^a \to R \to R/\mathfrak{m}^a \to 0$ and localize to get $\mathfrak{m}^a \otimes_R R_{\mathfrak{m}} \to R_{\mathfrak{m}} \to (R/\mathfrak{m}^a)_{\mathfrak{m}} = R/\mathfrak{m}^a \to 0$, so $R_{\mathfrak{m}}/\mathfrak{m}^aR_{\mathfrak{m}} \cong R/\mathfrak{m}^a$. □

At this point, we know all lcosed subvarieties (prime ideals in $\mathbb{C}[x,y]$) Y of $\mathbb{A}^2_{\mathbb{C}}$.

For example, we know $0 \leq \dim(Y) \leq 2$. If $\dim(Y) = 2$, then $Y = \mathbb{A}^2_{\mathbb{C}}$ corresponding to (0). If $\dim(Y) = 1$, then the codimension of prime is 1, then since $\mathbb{C}[x,y]$ is a UFD, then $p = (f)$ with $f \in \mathbb{C}[x,y]$ irreducible. If $\dim(Y) = 0$, then since $P \subseteq \mathbb{C}[x,y]$ is maximal, by Nullstellensatz, $P = (x-a, y-b)$ for some $a, b \in \mathbb{C}^2$.

Lemma 11.49 (Prime Avoidance)**.** Let $n \geq 1$ and $I_1, \cdots, I_n$, J be ideals in a commutative ring R. Suppose that all but at most one of the I_a's are prime. If $J = \bigcup_{a=1}^{n} I_a$, then J is contained in I_a for some a.

Proof. Use induction on n. Then $n = 1$ case is trivial. Suppose $n \geq 2$, and the statement holds for $n-1$. We can assume I_n is prime. Also, we can assume that J is not contained in the union of any $n-1$ of the I_a's or else by induction. So for each $1 \leq a \leq n$ we can choose $x_a \in J\backslash \bigcup_{b\neq a} I_b$. Clearly, $x_a \in I_a$. Consider $y = x_1 \cdots x_{n-1} + x_n$. This is in J so it must be in some I_a. But if $1 \leq a \leq n-1$, then $x_1 \cdots x_{n-1}$ is in I_a but $x_n \notin I_a$, $y \notin I_a$. Thus, $a = n$. Therefore, $y \in I_n$, but since I_n is prime, one of $x_1, \cdots, x_{n-1} \in I_n$, contradiction. Hence, $J \subseteq I_a$ for some a. □

Lemma 11.50. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. The dimension of R is the smallest number such that there are $f_1, \cdots, f_r \in \mathfrak{m}$ with $\mathfrak{m} = \mathbf{rad}(f_1 \cdots f_r)$.

Example 11.51. $R = \mathbb{C}[x,y]/(xy)$. It looks like $xy = 0$ cuts out closed points in $\mathbb{C}[x]/(x-y)$, but $\mathbb{C}[x,y]/(xy, x-y) \cong \mathbb{C}[x]/(x)^2$ is not $\mathbb{C}$. In R, $(x-y)$ is not maximal, but $\sqrt{(x-y)}$ is maximal.

Proof. We will make use of the corollary of Krull's principal ideal theorem. If $\mathbf{rad}(f_1, \cdots, f_r) = \mathfrak{m}$, then the codimension of $\mathfrak{m}$ is at most r, that is $\dim(R) \leq r$.

Conversely, if we let $r = \dim(R)$, we want to find r elements of $\mathfrak{m}$, and $f_1, \cdots, f_r$ such that $\mathfrak{m} = \mathbf{rad}(f_1, \cdots, ff_2)$. It (by induction) suffices to show that for any Noetherian local ring R of dimension > 0, then there is an element $f \in \mathfrak{m}$ with $\dim(R/(f)) \leq \dim(R) - 1$.

We now prove this statement. If an element $f \in \mathfrak{m}$ is not in any minimal prime ideal of R, then $\dim(R/(f)) \leq \dim(R) - 1$. Indeed, for any maximal chain of primes in R, we have $P_0 \subsetneq \cdots \subsetneq P_r$. Therefore, P_0 is minimal, so any chain of prime ideals in $R/(f)$ has length at most $r-1$. Geometrically, we can always find functions in $\mathbf{Spec}(R)$ that vanishes at a point but not at an entire irreducible component of $\mathbf{Spec}(R)$ since $\dim(R) > 0$, the maximal ideal is not prime. By prime avoidance lemma, since $\mathfrak{m}$ is not contained in any minimal prime in R, so $\mathfrak{m}$ is not contained in the union of minimal primes, and therefore we can find the f required. □

Definition 11.52. A system of parameters in a Noetherian local ring R means a sequence of elements $f_1, \cdots, f_r \in \mathfrak{m}$ such that $r = \dim(R)$ and $\mathbf{rad}(f_1, \cdots, f_r) = \mathfrak{m}$.

Every local Noetherian ring has a system of parameters.

In fact, when the ring is regular, we can get $\mathfrak{m} = (f_1, \cdots, f_r)$ without the radical.

Example 11.53 (Example of Regular Local Rings)**.** Any field is a regular local ring of dimension 0.

Any DVR such as $\mathbb{Z}_{(p)}$ for a prime p, or its completion, the p-adic integers given by $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n$. Then $\dim_{\mathbb{Z}/p}((p)/(p^2)) = 1$.

Example 11.54. $K[x_1, \cdots, x_n]$ is a regular local ring of dimension n, as its completion $k\left[[x_1, \cdots, x_n]\right]$, the power series ring.

Lemma 11.55. Let R be a Noetherian local ring. For any $f \in \mathfrak{m}$, $\dim(R/(f)) \geq \dim(R) - 1$. For any $f \in R$ which is not a zero divisor, $\dim(R/(f)) = \dim(R) - 1$.

Proof. Let $f \in \mathfrak{m}$, $r = \dim(R)$, $s = \dim(R)/(f)$, then we can choose a system of parameters $g_1, \cdots, g_s \in R/(f)$, then $R/(f)/(g_1, \cdots, g_s)$ is a local ring of dimension 0. Because $\mathfrak{m}$ is nilpotent, $\operatorname{rad}(f, g_1, \cdots, g_s) = \mathfrak{m}$, so $s + 1 \geq \dim(R)$, so $\dim(R/(f)) \geq \dim(R) - 1$. Now let f be a non-zero divisor. A non-zero divisor vanishes at $\mathfrak{m}$ but not any irreducible component: this shortens the chain of irreducible components. This holds if f is not contained in any minimal prime of R. Let $p_1, \cdots, p_s$ be the minimal primes in R. Suppose $f \in p_1$, we have a contradiction. For each $2 \leq j \leq s$, there is an element of p_j not in p_1 since p_1 is prime, the product of these $s-1$ elements in $p_2 \cap \cdots \cap p_s$, but not in p_1. Therefore, $fg_1 \in p_1 \cap \cdots \cap p_s = \operatorname{rad}(0) \subseteq R$, so there is a positive integer n such that $f^n g_1^n = 0$. Then f is a zero-divisor since $g_1 \neq 0$, contradiction. We conclude that f is not in a minimal prime ideal, so we $\dim(R/(f)) = \dim(R - 1)$. □

Proposition 11.56. A regular local ring is a domain.

Proof. We use induction on $r = \dim(R)$. If $r = 0$, then $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = \dim(R) = 0$, by Nakayama Lemma, $\mathfrak{m} = 0$, so R is a field. Now let R be regular local of dimension $r > 0$. We know that $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = r$ and in particular $\mathfrak{m}/\mathfrak{m}^2 \neq 0$, so $\mathfrak{m} \neq \mathfrak{m}^2$. By prime avoidance lemma, if $\mathfrak{m}$ were contained in the union of $\mathfrak{m}^2$ and the minimal primes of R, then it would be contained in one of these ideals. This is impossible since maximal ideal cannot be contained in minimal prime if $\dim(R) > 0$. Therefore, there is an element $f \in \mathfrak{m}$ not in $\mathfrak{m}^2$ and not in any minimal prime of R. By the proof of the previous result, $\dim(R/(f)) = \dim(R) - 1$. Let $S = R/(f)$. The maximal ideal $\mathfrak{m}_s$ has $\dim_K(\mathfrak{m}_s/\mathfrak{m}_{s^2}) = r-1$ because $(\mathfrak{m}_s/\mathfrak{m}_{s^2}) = (\mathfrak{m}/\mathfrak{m}^2)/(f)$ and $f \neq 0$ in $\mathfrak{m}^2$. Hence S is regular and we can apply the inductive hypothesis. S is a domain, so (f) is prime in R. Therefore, (f) contains some minimal prime ideal $p_1 \subseteq R$, but f is not contained in any minimal prime since any element in p_1 can be written as $y = fz$, hence $z \in p_1$, so $p_1 = \mathfrak{m}p_1$ (as $f \in \mathfrak{m}$). By Nakayama Lemma, $p_1 = 0$, so R is a domain. □

Definition 11.57. A regular sequence in a commutative ring R is a sequence $f_1, \cdots, f_n \in R$ such that f_1 is not a zero divisor in R, f_2 is not a zero divisor in $R/(f_1)$, f_3 is not a zero divisor in $R/(f_1, f_2)$, and so on.

Theorem 11.58. Let R be a Noetherian local ring. Then R is regular if and only if $\mathfrak{m}$ is generated by a regular sequence.

Remark 11.59. By homological algebra, this leads to a Noetherian local ring R is regular if and only if R has finite global dimension (any finitely-generated module has a resolution of finite length).

Remark 11.60 (Serre, 1956)**.** For a regular local ring R, $p \subseteq R$ prime, then R_p is also regular.

Remark 11.61 (Auslander-Buchsbaum, 1959)**.** Every regular local ring is UFD.

12 Completion and Filtration

Let R be a domain and $p \in \mathbf{Spec}(R)$. Note $R_p \subseteq \mathrm{Frac}(R)$ and $\mathrm{Frac}(R_p) = \mathrm{Frac}(R_p)$. Now R_p remembers the whole fractional field R. One can show that if X, Y are two structures with the same fractional field, then they are very close to be isomorphic.

Definition 12.1. For M an R-module, and I is an ideal of the ring R. We say that a filtration $M = M_0 \supseteq M_1 \supseteq$ is an I-filtration if we have that $IM_n \supseteq IM_{n+1}$, and it is stable if $IM_n = M_{n+1}$ for sufficiently large n.

Lemma 12.2. A stable I-filtration on M defines the same topology on M as the I-adic one, in particular there is an integer n_0 so that $M_{n+n_0} \subseteq I^n M$ and $I^{n+n_0} M \subseteq M_n$ for all $n \geq 0$.

Definition 12.3. Given a ring R and an ideal I, we get a topology by taking $R \supseteq I \supseteq I^2 \supseteq \cdots$, this is the I-adic topology. R is a topological ring with respect to this topology, and $\hat{R}_I(\hat{R})$ is the I-adic completion of R.

Example 12.4. $\varprojlim_n \mathbb{Z}/p^n = \mathbb{Z}/p$ as the p-adics.

Remark 12.5. Given a ring R and ideal I. We form a graded ring R^* by $R^* = \sum_i I^i$. Similarly, given an R-module M with an I-filtration, we get $M^* = \sum M_n$, since $I^m M_m \supseteq M_{n+m} M^*$ is graded R^*-module.

Lemma 12.6. Let R be a Noetherian ring. I is an ideal in R, and let M be a finitely-generated R-module with an I-filtration (M_n). Then we have M^* as a finitely-generated R^*-module if and only if the filtration is stable.

Lemma 12.7 (Artin-Rees)**.** Let R be a Noetherian ring, I an ideal in R. Let M be a finitely-generated R-module with an I-stable filtration (M_n) and M' is a submodule. Then $M' \cap M_n$ is an I-stable filtration, and the I-adic topology on M' coincides with the subspace topology induced by the I-adic topology on M.

Definition 12.8. A topological Abelian group is a topological space that is an Abelian group and where composition and inversion are continuous.

Remark 12.9. The topology of a topological Abelian group G is completely determined by the neighborhood of 0 (by translation).

Lemma 12.10. Let G be a topological Abelian group and let H be the intersection of all neighborhoods of 0. Then

1. H is a subgroup.
2. H is the closure of 0.
3. G/H is Hausdorff.
4. G is Hausdorff if and only if $H = 0$.

Remark 12.11. Let G be a local base at 0 consisting of nested subgroups, i.e. $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$. A typical example is the p-adic topology on $\mathbb{Z}$. A metric on the topological space is $d(x, y) = 2^{-v_p(x-y)}$. Then a local base of 0 is $\mathbb{Z} \supseteq p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq \cdots$, these subgroups $G_n = p^n\mathbb{Z}$ are clopen. Note that $\bigcup_{h \notin G_n} (h + G_n)$ is open and is the complement of G_n, so G_n is closed.

Definition 12.12. A Cauchy sequence is a sequence of elements $x_1, x_2, \cdots$ such that for any neighborhood U of 0, the sequence has the property that $x_n - x_m \in U$ for large enough n, m.

Take the image of the sequence in G/G_n is eventually constant, say equal to y_n, then there exists a map $G/G_{n+1} \to G/G_n$ that maps $y_{n+1} \mapsto y_n$. Taking the direct limit, we have $\varprojlim G/G_i$. In particular, we denote $\hat{G} = \varprojlim_i G/G_i$.

Corollary 12.13. Let R be a Noetherian ring. Given a finite short exact sequence $0 \to L \to M \to N \to 0$ of R-modules, then $0 \to \hat{L} \to \hat{M} \to \hat{N} \to 0$ is also a short exact sequence, and is of $\hat{R}$-modules.

Proposition 12.14. For R Noetherian, $\hat{R}$ is flat as an R-algebra.

Proposition 12.15. Let R be a Noetherian ring and I an ideal, and let $\hat{R}$ be its I-adic completion, then

1. $\hat{J} = \hat{R}J = \hat{R} \otimes_R J$.
2. $\hat{J^n} = \hat{J}^n$.
3. $\hat{I}$ is in the Jacobson radical of $\hat{R}$.

Proposition 12.16. For a ring R and a finite module M, $\varphi : \hat{R} \otimes_R M \to \hat{R} \otimes_R \hat{M}$ is surjective. In particular, if R is Noetherian, then the map is also injective.

We aim to show that if R is Noetherian, then the I-adic completion of R is also Noetherian.

Definition 12.17. Given a ring R with the I-adic filtration, we can form the associated grading ring of this filtration, defined as $G(R) = \bigoplus_{i=0}^{\infty} I_n/I_{n+1}$.

Given a module with an I-filtration, we can form the associated graded module $G(M)$, and this is a graded module over $G(R)$.

Proposition 12.18. Let R be Noetherian and I be an ideal of R. Then

1. $G(R)$ is Noetherian.
2. $G(R)$ and $G(\hat{R})$ are isomorphic as rings.
3. If M is a finite R-module and $\{M_n\}$ is a stable I-filtration, then $G(M)$ is a finite $G(R)$-module.

Lemma 12.19. Suppose $\varphi : M \to N$ to be a homomorphism of filtered modules. Then if $G(\varphi) : G(M) \to G(N)$ is injective (respectively, surjective), then the completion map $\hat{\varphi} : \hat{M} \to \hat{N}$ is injective (respectively, surjective).

Proposition 12.20. Let R be a ring and I as its ideal, and M be a R-module. Let (M_n) be an I-filtration. Suppose R is an I-adically complete and M is Hausdorff in the I-adic topology, and $G(M)$ is a finite $G(R)$-module, then M is a finite R-module.

Corollary 12.21. Under the hypotheses of the previous proposition, and suppose $G(M)$ is Noetherian as a $G(R)$-module, then M is also a Noetherian R-module.

Proof. We need to show that all submodules of M are finite. Let M' be a submodule and give it the induced filtration. Then the embedding $(M'_n) \to (M_n)$ gives the embedding $G(M') \to G(M)$, so $G(M')$ is finitely-generated $G(R)$-module and M' is complete (since M is complete), so M' is finitely-generated. □

Corollary 12.22. If R is a Noetherian ring, then $\hat{R}$ is Noetherian.

Proof. $G(\hat{R})$ is Noetherian, then apply the proposition above to the case where $R = \hat{R}$ and $M = \hat{R}$. □