Math 215A Lecture Notes
Prof. Burt Totaro
Fall 2018

Contents

Convention: All rings are commutative.

1 Basic Results

Lemma 1.1. *Let $f\colon A \longrightarrow B$ be a ring homomorphism, $\mathfrak{p} \subseteq B$ a prime ideal. Then $f^{-1}[\mathfrak{p}] \subseteq A$ is a prime ideal.*

Proof. We have that $B/\mathfrak{p}$ is a domain. Furthermore, $f^{-1}[\mathfrak{p}]$ is the kernel of the composition

$$A \longrightarrow B \longrightarrow B/\mathfrak{p}$$

Thus $A/f^{-1}[\mathfrak{p}]$ is isomorphic to the image of the composition, which is a subring of the domain $B/\mathfrak{p}$ and is therefore a domain. □

Remark. The same does not hold for maximal ideals. Indeed, $0 \subseteq \mathbb{Q}$ is a maximal ideal but its preimage under the inclusion $\mathbb{Z} \longrightarrow \mathbb{Q}$ is 0, which is not maximal in $\mathbb{Z}$.

Theorem 1.2. *Every nonzero ring contains a maximal ideal.*

Proof. Let A be a nonzero ring. Consider $S = \{I \subsetneq A : I \text{ is an ideal}\}$ This is nonempty as because $A \neq 0$, $0 \in S$. One must then check that the union of a chain of ideals is an ideal. Such a union is not the whole of A as none of the ideals contains a unit, lest they be the whole of A. Thus, by Zorn's lemma, S contains a maximal element, i.e. a maximal ideal. □

Corollary 1.2.1. *Let A be a ring, $I \subsetneq A$ an ideal. Then I is contained in some maximal ideal.*

Proof. Apply the above to A/I and use the order preserving correspondence between ideals of A/I and ideals of A containing I. □

2 The Prime Spectrum

Definition 2.1. Let A be a ring. We define $\operatorname{Spec}(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ is a prime ideal}\}$.

Definition 2.2. Let $I \subseteq A$ an ideal. We define $V(I) = \{\mathfrak{p} \in \operatorname{Spec}(A) : I \subseteq \mathfrak{p}\}$.

This is called the *prime spectrum* of A, or simply the *spectrum*. We introduce the *Zariski topology* on the prime spectrum whose closed subsets are precisely the $V(I)$. We would like to describe the ring homomorphisms from A to k for all fields k. Indeed, for $f\colon A \longrightarrow k$, the kernel of this is a prime ideal of A. Conversely, all prime ideals arise in this way. Indeed, for $\mathfrak{p} \in \operatorname{Spec}(A)$, we have that $\mathfrak{p}$ is the kernel of

$$A \longrightarrow A/\mathfrak{p} \longrightarrow \operatorname{Frac}(A/\mathfrak{p})$$

Example. Consider $\operatorname{Spec}\mathbb{Z} = \{(0), (2), (3), (5), (7), \dots\}$. Homomorphisms $\mathbb{Z} \longrightarrow k$ will necessarily factor through one of the above, which is $\mathbb{Z}/(p)$ for p prime or $\mathbb{Q}$ for 0. We also have the following picture of $\operatorname{Spec}\mathbb{Z}$.

Definition 2.3. For $f_1, \dots, f_r \in A$, let $\{f_1 = 0, \dots, f_r = 0\}$ denote $V((f_1, \dots, f_r))$.

Example. $\{12 = 0\} = \{(2), (3)\}$, which correspond to the fields where $12 = 0$.

Theorem 2.1. *The Zariski topology is a topology.*

Proof. The only tricky part is to prove that $V(I \cap J) \subseteq V(I) \cup V(J)$. Indeed, let $\mathfrak{p} \in V(I \cap J)$. If $\mathfrak{p} \notin V(I) \cup V(J)$ then there are $a \in I - \mathfrak{p}$ and $b \in J - \mathfrak{p}$. Then $ab \in I \cap J \subseteq \mathfrak{p}$. However, as $\mathfrak{p}$ is prime, $ab \notin \mathfrak{p}$. □

Theorem 2.2. *Let $f\colon A \longrightarrow B$ a ring homomorphism. Define*

$$\operatorname{Spec}(f)\colon \operatorname{Spec}(A) \longrightarrow \operatorname{Spec}(B)$$

via $\mathfrak{p} \mapsto f^{-1}[\mathfrak{p}]$. Then this is continuous. Furthermore, the map

$$\operatorname{Spec}(A/I) \longrightarrow \operatorname{Spec}(A)$$

is a homeomorphism to the closed subset $V(I)$.

Proof. Let $g = \operatorname{Spec}(f)$. We show that g pulls back closed sets to closed sets. Let $J = (f[I])$. We claim that $g^{-1}[V(I)] = V(J)$. Indeed,

$$\mathfrak{p} \in g^{-1}[I] \iff g(\mathfrak{p}) \in V(I) \iff f^{-1}[\mathfrak{p}] \in V(I) \iff$$

$$I \subseteq f^{-1}[\mathfrak{p}] \iff f[I] \subseteq \mathfrak{p} \iff J \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(J)$$

So g is indeed continuous.
Let g be the map $\operatorname{Spec}(A/I) \longrightarrow \operatorname{Spec}(A)$. g is a bijection onto $V(I)$ by correspondence. It

is continuous as above, so we must show that it is a closed map. Let $J \subseteq A/I$ an ideal, and let $K \subseteq A$ be its inverse image. Then

$$\mathfrak{p} \in g[V(J)] \iff \mathfrak{p} = g(\mathfrak{q}) \text{ for some } \mathfrak{q} \supseteq J \text{ prime} \iff K \subseteq \mathfrak{p}$$

so $g[V(J)] = V(K)$. □

Theorem 2.3. *Let A be a ring. Recall the nilradical* $\operatorname{nil} A = \{x \in A : \exists n \geq 1 \text{ s.t. } x^n = 0\}$. *Then* $\operatorname{nil} A = \bigcap \operatorname{Spec} A$.

Proof. "$\subseteq$": Let $a \in \operatorname{nil} A$. Then some $a^n = 0$. Let $\mathfrak{p} \in \operatorname{Spec} A$. Then in the domain $A/\mathfrak{p}$, $a^n = 0$, so $a = 0$, so $a \in \mathfrak{p}$.
"$\supseteq$": Let $a \notin \operatorname{nil} A$. We find a prime ideal that does not contain a. Let S be the set of all ideals that contain no power of a. By assumption, $0 \in S$. Then by Zorn's lemma, there is a maximal element $\mathfrak{p} \in S$. We claim that $\mathfrak{p}$ is prime. $x \notin \mathfrak{p}$ so $\mathfrak{p} \neq A$. Furthermore, let $x, y \notin \mathfrak{p}$. We claim $xy \notin \mathfrak{p}$. As $x \notin \mathfrak{p}$, $(x) + \mathfrak{p} \notin S$ by maximality, so some $a^n \in (x) + \mathfrak{p}$. Similarly, some $a^m \in (y) + \mathfrak{p}$. Then $a^{n+m} \in (xy) + \mathfrak{p}$ so $xy \notin \mathfrak{p}$. □

Corollary 2.3.1. *Let $I \subseteq A$ an ideal. Recall the radical of I* $\operatorname{rad} I = \{x \in A : \exists n \geq 1 \text{ s.t. } x^n \in I\}$. *Then* $\operatorname{rad} I = \bigcap V(I)$.

Proof. Observe that $\operatorname{rad}(I)$ is the inverse image of $\operatorname{nil}(A/I)$, which is $\bigcap \operatorname{Spec} A$ as above. Then we are done by correspondence. □

Theorem 2.4. *Let $I, J \subseteq A$ ideals. Then* $V(I) = V(J) \iff \operatorname{rad}(I) = \operatorname{rad}(J)$.

Proof. Indeed, if $V(I) = V(J)$ then we are done by the corollary. Conversely, let $\operatorname{rad}(I) = \operatorname{rad}(J)$. We claim that $I \subseteq \mathfrak{p} \iff \operatorname{rad}(I) \subseteq \mathfrak{p}$ for any prime $\mathfrak{p}$. Indeed, $I \subseteq \operatorname{rad}(I)$ so one direction is immediate. Conversely, if $I \subseteq \mathfrak{p}$ then $\operatorname{rad} I \subseteq \operatorname{rad} \mathfrak{p} = \mathfrak{p}$. Thus, $V(I) = V(\operatorname{rad} I)$ so $V(I) = V(J)$. □

This tells us that there is a one to one order reversing correspondence between radical ideals of A (those that are equal to their radical) and closed subsets of $\operatorname{Spec} A$ via $I \mapsto V(I)$.

Remark. We showed earlier that $V(I \cap J) = V(I) \cup V(J)$. We show now that $V(IJ) = V(I) \cup V(J)$.

Proof. By the theorem, it suffices to show that $\operatorname{rad}(IJ) = \operatorname{rad}(I \cap J)$. We know $IJ \subseteq I \cap J$ so $\operatorname{rad}(IJ) \subseteq \operatorname{rad}(I \cap J)$. Conversely, let $x \in I \cap J$. Then $x^2 \in IJ$ so $x \in \operatorname{rad}(IJ)$. As rad is order preserving and idempotent, we therefore have $\operatorname{rad}(I \cap J) \subseteq \operatorname{rad}(IJ)$. □

3 Irreducible Closed Subsets of $\operatorname{Spec} A$

Lemma 3.1. *Let A be a domain. Then the closure of* $\{0\}$ *in* $\operatorname{Spec} A$ *is* $\operatorname{Spec} A$, *i.e.* $\{0\}$ *is dense in* $\operatorname{Spec} A$. *We call this the generic point of* $\operatorname{Spec} A$.

Proof. Let I be an ideal such that $\{0\} \subseteq V(I)$, i.e. $0 \in V(I)$. Then $I \subseteq 0$, so $I = 0$. Then $V(I) = \operatorname{Spec} A$. Thus, $\overline{\{0\}} = \operatorname{Spec} A$. □

Definition 3.1. A nonempty topological space X is called irreducible if it cannot be written as the union of two closed subsets that are not the whole of X.

This is a very strong notion. Indeed, a space being irreducible certainly implies that it is connected. However, the converse it not true. Indeed, consider $\mathbb{R} = (-\infty, 0] \cup [0, \infty)$.

Lemma 3.2. *A closed subset of* $\operatorname{Spec} A$ *is irreducible if and only if it is the closure of a point. Then there are one to one correspondences between primes in* A*, points in* $\operatorname{Spec} A$*, and irreducible closed subsets of* $\operatorname{Spec} A$*.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$. Let $S = \overline{\{\mathfrak{p}\}}$. Certainly, S is nonempty. Now, let $S = T_1 \cup T_2$ be closed subsets. Then $\mathfrak{p} \in T_1$ or $\mathfrak{p} \in T_2$. Without loss of generality, say $\mathfrak{p} \in T_1$. Then $S = T_1$ so S is irreducible. Note that this proof works for any topological space, i.e. the closure of any point is irreducible.
Conversely, let S be an irreducible closed subset of $\operatorname{Spec} A$. Then $S = V(I)$ for some ideal I. Without loss of generality, I can be assumed to be radical. We claim that it is prime. Then as the closure of a prime ideal $\mathfrak{p}$ is $V(\mathfrak{p})$, we will be done. Indeed, $I \neq A$ as S is irreducible therefore nonempty. Now, let $xy \in I$. Suppose neither x nor y is in I. Then let $T_1 = V(I + (x)), T_2 = V(I + (y))$. Then $T_i \subsetneq S$, $i = 1, 2$ as $\operatorname{rad}(I + (x)) \neq I = \operatorname{rad}(I)$. We claim then that $T_1 \cup T_2 = S$. Indeed,

$$\begin{aligned} T_1 \cup T_2 &= V(I + (x)) \cup V(I + (y)) \\ &= V((I + (x))(I + (y))) \\ &= V(I + (xy)) \\ &= V(I) \\ &= S \end{aligned}$$

which contradicts the irreducibility of S. □

4 Modules

Note that the Hom sets in **Ring** are just sets. However, in **R-Mod**, they are themselves R-modules. The idea is to "linearize" ring theory, in the way that vector bundles linearize topology or representations linearize group theory.

Remark. An R-action on an abelian group M is equivalent to a map $R \longrightarrow \operatorname{End}_{\mathbf{Ab}}(M)$, which is a noncommutative ring in general.

Definition 4.1. Let M be an R-module. We define the annihilator

$$\operatorname{Ann}_R(M) = \{a \in R : am = 0 \ \forall m \in M\}$$

which is easily checked to be an ideal.

Definition 4.2. Let $\{M_i\}_{i \in I}$ be a set of R-modules. We define

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \in \prod_{i \in I} M_i : m_i = 0 \text{ for all but finitely many } i\}$$

endowed with pointwise R-module operations. As a special case we define

$$R^{\oplus I} = \bigoplus_{i \in I} R$$

which is called the free R-module on I. Indeed, this is free in the categorical sense, i.e. there is a natural bijection

$$\{f \colon I \longrightarrow M\} \longleftrightarrow \{R\text{-linear maps } R^{\oplus I} \longrightarrow M\}$$

This means that it satisfies the following universal property:
Given any set map $I \longrightarrow M$, we have

$$\begin{array}{ccc} I & \longrightarrow & R^{\oplus I} \\ & \searrow & \downarrow \exists! \\ & & M \end{array}$$

with the map $I \longrightarrow R^{\oplus I}$ defined via $i \mapsto e_i$ the i^{th} basis vector of $\prod_{i \in I} R$, and the induced map R-linear.

This is an important notion because all modules are quotients of free modules. Indeed, for an R-module M, there is a surjection $R^{\oplus M} \longrightarrow M$ which lifts the identity on M. We write this as an exact sequence

$$R^{\oplus I} \longrightarrow M \longrightarrow 0$$

This mimics the case in group theory, where all groups are quotients of free groups. Indeed, we also have the notion of the presentation of a module.

Definition 4.3. A presentation of an R-module M is an exact sequence

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

which says that $M \cong \operatorname{cok}(R^{\oplus J} \longrightarrow R^{\oplus I})$. Then M is determined by a map between free R-modules, which, as in linear algebra, can be thought of as a matrix.

Lemma 4.1. *Every R-module has a presentation.*

Proof. Let M be an R-module. As above, we have an exact sequence

$$R^{\oplus I} \longrightarrow M \longrightarrow 0$$

The kernel of this map is also an R-module, and is therefore also a quotient of a free R-module $R^{\oplus J}$. This yields a presentation

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

□

As in the case of groups, this gives us a recipe to define R-modules. For example, we can define via presentation the $\mathbb{Z}$-module $\mathbb{Z} < e_1, e_2 | 2e_1 = 2e_2 >$, which is the cokernel of the map $\mathbb{Z} \longrightarrow \mathbb{Z}^2$ via $1 \mapsto (2, -2)$. One can check that this is in fact $\mathbb{Z} \oplus \mathbb{Z}/(2)$.

Definition 4.4. An R-module M is called projective if it is a direct summand of a free module.

Lemma 4.2. *Let M be an R-module. The following are equivalent.*

1. *M is projective.*
2. *Any exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow M \longrightarrow 0$ splits.*
3. *For any exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, any map $M \longrightarrow C$ lifts to a map $M \longrightarrow B$, i.e. we have*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & & & \nwarrow & \uparrow & & \\ & & & & & & M & & \end{array}$$

Proof. 2) $\implies$ 1). Consider the exact sequence

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

which splits by assumption, so $R^{\oplus I} = \ker(f) \oplus M$, so M is projective.
3) $\implies$ 2). We have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & M & \longrightarrow & 0 \\ & & & & & \nwarrow & \uparrow{\scriptstyle \mathrm{id}} & & \\ & & & & & & M & & \end{array}$$

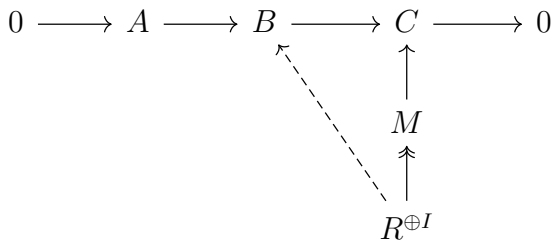
which is precisely a splitting.
1) $\implies$ 3). Let $M \oplus N = R^{\oplus I}$. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & & & & \uparrow & & \\ & & & & & & M & & \end{array}$$

We desire a lift $M \longrightarrow B$. Indeed, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & & & & \uparrow & & \\ & & & & & & M & & \\ & & & & & & \uparrow\uparrow & & \\ & & & & & & R^{\oplus I} & & \end{array}$$

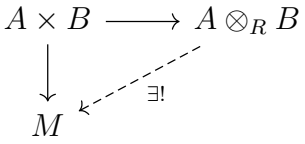
By freeness we get



And the restriction of this map to M yields the desired lift. □

5 Tensor Products

Definition 5.1. Let A and B be R-modules. We define the tensor product of A and B to be an R-module $A \otimes_R B$ along with an R-bilinear map $A \times B \longrightarrow A \otimes_R B$ that is universal, i.e. for any R-bilinear map $A \times B \longrightarrow M$, we have the following commutative diagram



with the induced map R-linear.

Lemma 5.1. *The tensor product of two R-modules exists.*

Proof. First, write the basis elements of $R^{\oplus A \times B}$ as $a \otimes b$. One can show that

$$A \otimes_R B = \frac{R^{\oplus A \times B}}{\left(\left\{ \begin{array}{l} (a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b \\ a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2 \\ (ra) \otimes b = r(a \otimes b) \\ a \otimes (rb) = r(a \otimes b) \end{array} \middle| \, a_1, a_2, a \in A, b_1, b_2, b \in B \right\} \right)}$$

satisfies the desired universal property, with the map $A \times B \longrightarrow A \otimes_R B$ defined as the composition $A \times B \longrightarrow R^{\oplus A \times B} \longrightarrow A \otimes_R B$. □

Remarks. 1. Elements of $M \otimes_R N$ look like $\sum_{i=1}^{n} r_i(m_y \otimes n_i)$. The r_i can be omitted using the above relations. This is in general not a unique representation.

2. It is hard to tell when an element of $M \otimes_R N$ is 0. For example, in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$, we have

$$\begin{aligned} 1 \otimes 1 &= \left(2 \cdot \frac{1}{2}\right) \otimes 1 \\ &= \frac{1}{2} \otimes 2 \\ &= \frac{1}{2} \otimes 0 \\ &= 0 \end{aligned}$$

3. In the case of R noncommutative, we can still define a tensor product of a right R-module A and a left R-module B. We must rewrite the relations above to instead say $(ar) \otimes b = a \otimes (rb)$. However, this does not yield the structure of an R-module, and is only an abelian group.

4. When it is clear from context we omit the subscript R.

Lemma 5.2. *Let $M, N, P, \{N_i\}_{i \in I}$ be R-modules.*

1. $M \otimes N \cong N \otimes M$
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$
3. $R \otimes M \cong M$
4. $M \otimes \bigoplus_{i \in I} N_i \cong \bigoplus_{i \in I} M \otimes N_i$

with all isomorphisms canonical.

Remark. Point 4. in the lemma is actually a consequence of the more general fact that the functor $- \otimes M$ is left adjoint to $\mathrm{Hom}(M, -)$ and is therefore cocontinuous. In particular, as the direct sum is the coproduct in $\mathbf{R - Mod}$, point 4. follows.

Lemma 5.3. *Let*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be exact and let M be an R-module. Then

$$A \otimes M \xrightarrow{f \otimes id} B \otimes M \xrightarrow{g \otimes id} C \otimes M \longrightarrow 0$$

is exact.

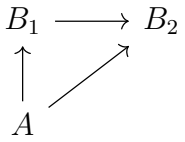
Proof. Surjectivity of $g \otimes$id is immediate from surjectivity of g. For exactness at $B \otimes M$, prove that for any R-module N, there is a one to one correspondence between maps $C \otimes M \longrightarrow N$ and maps $B \otimes M \longrightarrow N$ that vanish on $A \otimes M$, then use Yoneda's lemma. □

Remark. This is not true for $0 \longrightarrow A \longrightarrow B$. Indeed, take the exact sequence of $\mathbb{Z}$ modules $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$.
We tensor this with $\mathbb{Z}/(2)$ to get the sequence $0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/(2) \xrightarrow{*2} \mathbb{Z} \otimes \mathbb{Z}/(2)$. This map is actually the 0 map and is therefore not injective, so the sequence is no longer exact.

Example. Applying the lemma to $R \xrightarrow{\cdot f} R \longrightarrow R/(f) \longrightarrow 0$, we tensor this with an R-module M to get the exact sequence $M \xrightarrow{\cdot f} M \longrightarrow M \otimes R/(f) \longrightarrow 0$. This allows us to compute the tensor product of any two finitely generated modules over a PID by the structure theorem.

6 Algebras and Tensor Products

Definition 6.1. Let A be a ring. An A-algebra is a ring B with a ring homomorphism $A \longrightarrow B$. This induces an A-module structure on B. An $A-algebra$ homomorphism $B_1 \longrightarrow B_2$ is a ring homomorphism such that



commutes.

Remarks. 1. $\mathbb{Z}$ is initial in **Ring**, so $\mathbb{Z}$-algebras are just rings, like how $\mathbb{Z}$-modules are just abelian groups.

2. The polynomial ring $A[S]$ is the free A-algebra on S.

Definition 6.2. An A-algebra B is said to be of finite type (as an A-algebra) if it is finitely generated as an A-algebra, i.e. if there exist elements $a_1, \ldots, a_n$ such that every element of B is a polynomial in the a_i. Equivalently, that there exists a surjection $A[x_1, \ldots, x_n] \longrightarrow B$.

Definition 6.3. An affine variety over a field k is $\operatorname{Spec} R$ for some R a domain of finite type over k. We specifically define $\mathbb{A}^n_k = \operatorname{Spec}(k[x_1, \ldots, x_n])$.

For an A-algebra B, we look at two functors to look at. One is $B-Mod \longrightarrow A-Mod$ via restriction of scalars. Another is called extension of scalars, which is a functor $A-Mod \longrightarrow B-Mod$ via $M \mapsto M \otimes B$. By right exactness of the tensor product, extension of scalars preserves presentations. Indeed, take $M = \mathbb{Z} < e_1, e_2 | 2e_1, 2e_2 >$. Then

$$M \otimes \mathbb{Q} = \mathbb{Q} < e_1, e_2 | 2e_1, 2e_2 >= \mathbb{Q}$$

Furthermore, if B and C are A-algebras, then $B \otimes C$ is an A-algebra via $(b_1 \otimes b_2)(c_1 \otimes c_2) = b_1c_1 \otimes b_2c_2$, which is well defined by universal property. This extended linearly defined the desired ring structure.

7 Exactness of Tensor Products

As discussed above, it is not true that tensoring preserves all exact sequences. We want to consider when it is.

Definition 7.1. An R-module M is called flat if for every exact sequence $A \longrightarrow B \longrightarrow C$, the sequence $A \otimes M \longrightarrow B \otimes M \longrightarrow C \otimes M$ is exact.

For example, the $\mathbb{Z}$-module $\mathbb{Z}/(2)$ is not flat, as the sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$ is not exact when tensored with $\mathbb{Z}/(2)$.

Remark. Any free module in flat. Indeed,

$$\begin{aligned}(A \longrightarrow B \longrightarrow C) \otimes R^{\oplus I} &= A^{\oplus I} \longrightarrow B^{\oplus I} \longrightarrow C^{\oplus I} \\ &= (A \longrightarrow B \longrightarrow C)^{\oplus I}\end{aligned}$$

which is exact. More generally, one can show that any direct summand of a flat module is flat, so projective modules are flat. However, the converse is not true. Indeed, $\mathbb{Q}$ is not $\mathbb{Z}$-projective but is flat.

Lemma 7.1. *Let M be an R-module. The following are equivalent.*

1. *M is flat.*
2. *Tensoring by M preserves injections.*
3. *For any ideal I, tensoring by M preserves injectivity of the inclusion of I.*

Proof. 1) $\implies$ 2) $\implies$ 3) is immediate. 3) $\implies$ 1) is not, and we will delay this until we have the Tor functor. □

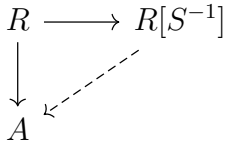
8 Localization and Local Rings

Definition 8.1. Let R be a ring. A subset $S \subseteq R$ is called multiplicative if it contains 1 and is closed under multiplication. In other words, it is a submonoid of the multiplicative monoid of R

Definition 8.2. Let $S \subseteq R$ be a multiplicative subset. We define the localization of R at S to be the ring $R[S^{-1}] = \left\{\frac{r}{s} : r \in R, s \in S\right\}$ where $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ if there is some $u \in S$ such that $u(r_1 s_2 - r_2 s_1) = 0$. The arithmetic on the localization is defined by $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$ and $\frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$. One may check that these operations are well defined and induce a ring structure.

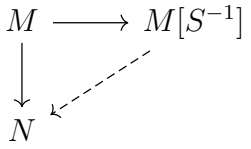
There is a canonical map $R \longrightarrow R[S^{-1}]$ via $r \mapsto \frac{r}{1}$. In $R[S^{-1}]$, we often write $r = \frac{r}{1}$. It is clear that localizing at S forces all elements of S to map to units under this map. This is, in fact, a universal property.

Lemma 8.1. *Let $S \subseteq R$ be a multiplicative subset. Let $R \longrightarrow A$ be a ring homomorphism sending S to the unit group of A. Then we have the following commutative diagram.*



Looking carefully at the definition of localization of a ring, we see that the numerator only requires multiplication of elements of R by elements of S. We need not multiply general elements of R by general elements of S. Indeed, this tells us that we can use the same construction to localize an R-module M at S. Indeed, this has a similar universal property, but we must reinterpret what it means for elements of S to become units. This condition becomes the map $M \xrightarrow{\cdot s} M$ is a bijection for all $s \in S$.

Lemma 8.2. *Let $S \subseteq R$ be a multiplicative subset, M, N R-modules. Suppose there is an R-linear map $M \longrightarrow N$ such that multiplication by elements of S is a bijection in N. Then we have the following.*

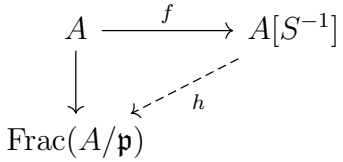


Examples. 1. Let $f \in A$. We define $A[1/f]$ to be the localization of A at the multiplicative subset $\{1, f, f^2, f^3, \dots\}$. Note that if f is nilpotent then this is the 0 ring. This is because localizing at 0 is always the 0 ring.

2. Let $\mathfrak{p}$ be a prime ideal of A. We define $A_{\mathfrak{p}}$ to be the localization of A at $A - \mathfrak{p}$.

Theorem 8.3. *Let $S \subseteq A$ a multiplicative subset. Then there is a one to one correspondence between* $\operatorname{Spec}(A[S^{-1}])$ *and* $\{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \cap S = \emptyset\}$

Proof. Let f be the canonical map $A \longrightarrow A[S^{-1}]$. Let $g\colon \operatorname{Spec}(A[S^{-1}]) \longrightarrow \operatorname{Spec} A$ be the induced map. We show first that g is one to one. Indeed, let $g(\mathfrak{p}) = g(\mathfrak{q})$. Observe that $\frac{a}{s} \in \mathfrak{p} \iff \frac{a}{1} \in \mathfrak{p} \iff a \in g(\mathfrak{p})$. Thus, $\mathfrak{p} = \mathfrak{q}$.
It is clear that $\operatorname{im}(g) \subseteq \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \cap S = \emptyset\}$. Conversely, let $\mathfrak{p} \in \operatorname{Spec} A$ such that $\mathfrak{p} \cap S = \emptyset$. We then have a map $A \longrightarrow \operatorname{Frac}(A/\mathfrak{p})$. As $\mathfrak{p} \cap S = \emptyset$, S maps to the units (i.e. the nonzero elements) of $\operatorname{Frac}(A/\mathfrak{p})$. Then by universal property, there is a map $h\colon A[S^{-1}] \longrightarrow \operatorname{Frac}(A/\mathfrak{p})$ such that



commutes. Let $\mathfrak{q} = h^{-1}[0]$. Then $g(\mathfrak{q}) = f^{-1}[\mathfrak{q}] = f^{-1}[h^{-1}[0]]$, which equals the pullback of 0 along the map $A \longrightarrow \operatorname{Frac}(A/\mathfrak{p})$ by commutativity of the diagram. This is, of course, the kernel of this map, which is $\mathfrak{p}$. Then $g(\mathfrak{q}) = \mathfrak{p}$, so g provides the desired correspondence. □

Examples. 1. $\operatorname{Spec}(A[1/f]) = \{\mathfrak{p} \in \operatorname{Spec}(A) : f \notin \mathfrak{p}\}$

2. $\operatorname{Spec}(A_{\mathfrak{p}}) = \{\mathfrak{q} \in \operatorname{Spec}(A) : \mathfrak{q} \subseteq \mathfrak{p}\}$

Definition 8.3. A ring is called local if it has exactly one maximal ideal. For a local ring A with maximal ideal $\mathfrak{m}$, we call $A/\mathfrak{m}$ the residue field of A.

Lemma 8.4. *A ring A is local if and only if $A - A^\times$ is an ideal.*

Proof. Let A be local with maximal ideal $\mathfrak{m}$. Then $A - A^\times$ is the union of all maximal ideals of A, which is of course just $\mathfrak{m}$, an ideal. Conversely, suppose $\mathfrak{m} = A - A^\times$ is an ideal. It is certainly maximal, as any ideal strictly containing it will contain a unit. Also, let $\mathfrak{n}$ be another maximal ideal. As it contains no units, we have $\mathfrak{n} \subseteq \mathfrak{m}$, so by maximality, $\mathfrak{n} = \mathfrak{m}$. Thus, A is local. □

Example. Let $A = k[[x_1, \ldots, x_n]]$. Then $A^\times = \{f \in A : f(0) \neq 0\}$, so $A - A^\times = \{f \in A : f(0) = 0\}$, which is an ideal so A is local. Indeed, $A - A^\times = (x_1, \ldots, x_n)$, so its residue field is k.

Of course, the term localization and the term local ring sound alike. We provide the connection in the following theorem.

Theorem 8.5. *The localization of a ring at a prime ideal is local.*

Proof. Let A be a ring, $\mathfrak{p}$ a prime ideal. By the correspondence above, we have that $\operatorname{Spec}(A_\mathfrak{p}) \cong \{\mathfrak{q} \in \operatorname{Spec} A : \mathfrak{q} \subseteq \mathfrak{p}\}$. This correspondence is also order preserving, so as the unique maximal element of $\{\mathfrak{q} \in \operatorname{Spec} A : \mathfrak{q} \subseteq \mathfrak{p}\}$ is $\mathfrak{p}$, there is a unique maximal element of $\operatorname{Spec}(A_\mathfrak{p})$, so $A_\mathfrak{p}$ is local. Furthermore, its maximal ideal is the ideal generated by $\mathfrak{p}$. □

Remark. The residue field of $A_\mathfrak{p}$ is $\operatorname{Frac}(A/\mathfrak{p})$.

Examples.
1. $\mathbb{Z}_{(p)}$ is local with residue field $Z/(p)$.
2. $\mathbb{C}[x]_{(x)}$ is local with residue field $\mathbb{C}$.
3. $\mathbb{C}[x, y]_{(x)}$ is local with residue field $\mathbb{C}(y)$.

Localizing an R-module M at S yields $M[S^{-1}]$, which is both an R-module and an $R[S^{-1}]$-module. Furthermore, we may localize functions. Indeed, localizing the R-homomorphism $M \xrightarrow{f} N$ at S yields an $R[S^{-1}]$-homomorphism $M[S^{-1}] \longrightarrow N[S^{-1}]$ via $\frac{m}{s} \mapsto \frac{f(m)}{s}$. This means that localization is a functor from **R-Mod** to $\mathbf{R[S^{-1}] - Mod}$. In fact, it's additive.

Theorem 8.6. *The functor* $S^{-1} \colon \mathbf{R - Mod} \longrightarrow \mathbf{R[S^{-1}] - Mod}$ *is exact.*

Proof. Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be exact. Its localization at S composes to 0 as the localization functor is additive. That means that $\operatorname{im}(f[S^{-1}]) \subseteq \ker(g[S^{-1}])$. Conversely, let $\frac{m}{s} \in \ker(g[S^{-1}])$. Then $\frac{g(m)}{s} = 0$. Then there exists $u \in S$ such that $ug(m) = 0$, so $g(um) = 0$, so $um \in \ker(g) = \operatorname{im}(f)$. Then there exists an $x \in M_1$ such that $f(x) = um$. Then $\frac{f(x)}{us} = \frac{um}{us} = \frac{m}{s}$, so $\ker(g[S^{-1}]) \subseteq \operatorname{im}(f[S^{-1}])$. □

Theorem 8.7. *There is a natural isomorphism between* $M[S^{-1}]$ *and* $M \otimes_R R[S^{-1}]$.

Proof. Indeed, the R-bilinear map $\left(m, \frac{r}{s}\right) \mapsto \frac{rm}{s}$ induces a map $M \otimes_R R[S^{-1}] \longrightarrow M[S^{-1}]$ by universal property. The map $M \longrightarrow M \otimes_R R[S^{-1}]$ via $m \mapsto m \otimes 1$ induces a map $M[S^{-1}] \longrightarrow M \otimes_R R[S^{-1}]$ via universal property, as S acts by bijections on $M \otimes_R R[S^{-1}]$. One can check that these are inverses. Then, one needs only check naturality in M, which is not hard to verify. □

Remark. Any localization of R is flat as an R-module. For example, $\mathbb{Q}$ is flat over $\mathbb{Z}$. Furthermore, by cocontinuity of the tensor product, localization is cocontinuous and therefore commutes with direct sums.

Examples.
1. Let M be the $\mathbb{Z}$-module $\mathbb{Z}^2 \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(8) \oplus \mathbb{Z}/(5)$. Localizing this at (0) yields $\mathbb{Z}^2_{(0)} \oplus (\mathbb{Z}/(2))_{(0)} \oplus (\mathbb{Z}/(8))_{(0)} \oplus (\mathbb{Z}/(5))_{(0)} = \mathbb{Q}^2$
2. The same method yields that $M_{(2)} = (\mathbb{Z}/(2))^2 \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$.

9 Local Properties

We say that a property of R-modules is *local* if it holds if and only if it holds at the localization at every prime ideal. This also often happens if and only if it holds at the localization at every maximal ideal.

Lemma 9.1. *Let M be an R-module. The following are equivalent.*

1. $M = 0$
2. $M_{\mathfrak{p}} = 0$ *for all* $\mathfrak{p}$ *prime.*
3. $M_{\mathfrak{m}} = 0$ *for all* $\mathfrak{m}$ *maximal.*

Which says that a module being 0 *is a local property.*

Proof. Certainly 1) $\implies$ 2) $\implies$ 3). Suppose then that 3) holds. Suppose that $M \neq 0$. As $x \neq 0$, $1 \notin \mathrm{Ann}_R(x)$, so $\mathrm{Ann}_R(x) \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. We claim then that $x \neq 0$ in $M_{\mathfrak{m}}$. Indeed, if it were 0, then there would exist a $u \notin \mathfrak{m}$ such that $ux = 0$. But then $u \in \mathrm{Ann}_R(x) \subseteq \mathfrak{m}$, contradiction. □

Lemma 9.2. *Let $f\colon M \longrightarrow N$ be R-linear. The following are equivalent.*

1. f *is injective.*
2. $f_{\mathfrak{p}}$ *is injective for all* $\mathfrak{p}$ *prime.*
3. $f_{\mathfrak{m}}$ *is injective for all* $\mathfrak{m}$ *maximal.*

Which says that being injective is a local property.

Proof. 1) $\implies$ 2). This follows from exactness of localization.
2) $\implies$ 3). Clear.
3) $\implies$ 1). If f was not injective then $\ker(f) \neq 0$, so as a module being 0 is local, there exists some maximal ideal $\mathfrak{m}$ such that $\ker(f)_{\mathfrak{m}} \neq 0$. This would yield the desired contradiction if $\ker(f)_{\mathfrak{m}} = \ker(f_{\mathfrak{m}})$. Indeed, consider the exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow M \longrightarrow N$$

By exactness of localization, we have an exact sequence

$$0 \longrightarrow \ker(f)_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$$

which yields the desired equality. □

Remark. The same proof applied to $\mathrm{cok}(f)$ shows that surjectivity is also local. Thus, bijectivity is local as well. This does not, however, say that modules being isomorphic is a local property, as the isomorphisms at each localization need not come from the isomorphism itself.

Definition 9.1. For a prime ideal $\mathfrak{p}$, we define the residue field of R at $\mathfrak{p}$ to be $\mathrm{Frac}(R/\mathfrak{p})$.

Definition 9.2. For an prime ideal $\mathfrak{p}$, and an R-module M, we define the fiber of M at $\mathfrak{p}$ to be $M \otimes_R (R/\mathfrak{p})$.

Remark. For $I \subseteq R$ an ideal, observe that $M \otimes_R (R/I) = M/IM$. Indeed, tensor the exact sequence $I \longrightarrow R \longrightarrow R/I \longrightarrow 0$ with M to yield the exact sequence (by right exactness of the tensor product) $I \otimes M \longrightarrow R \otimes M \longrightarrow R/I \otimes M \longrightarrow 0$, which becomes $IM \longrightarrow M \longrightarrow R/I \otimes M \longrightarrow 0$. Then by exactness, $M \otimes R/I = M/IM$.

Note that the local properties we described above do not necessarily generalize to being "fiber local". For example, we claim that there exists a nonzero $\mathbb{Z}$-module whose fiber at all prime ideals is 0. Indeed, take $\mathbb{Q}$. Then as $p\mathbb{Q} = \mathbb{Q}$, the fibers are all 0, but $\mathbb{Q} \neq 0$. There is, however, an approximation of this when dealing with finitely generated modules.

Theorem 9.3 (Nakayama's lemma)**.** *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. Then $M = 0$ if and only if its fiber at $\mathfrak{m}$ is 0, i.e. $M \otimes_R (R/\mathfrak{m}) = M/\mathfrak{m}M = 0$*

Proof. Of course, if $M = 0$ its fiber at $\mathfrak{m}$ is 0. Conversely, let $M = \mathfrak{m}M$. As M is finitely generated, let $x_1, \ldots, x_n \in M$ generate M. Let n be minimal. Suppose that $M \neq 0$. As $\mathfrak{m}M = M$, we have $x_n \in \mathfrak{m}M$. Then $x_n = a_1x_1 + \cdots + a_nx_n$, each $a_i \in \mathfrak{m}$. Thus, $(1 - a_n)x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}$. Furthermore, $1 - a_n \notin \mathfrak{m}$, so as R is local, $1 - a_n \in R^\times$. Then by dividing, x_n is an R-linear combination of $x_1, \ldots, x_{n-1}$, but n was chosen to be minimal. □

Remark. To fully realize this as a generalization of local properties, one can show that for any ring R and a finitely generated R-module M that $M = 0$ if and only if all fibers of M at the maximal ideals of R are 0. Indeed, we can apply Nakayama's lemma to each $R_\mathfrak{m}$-module $M_\mathfrak{m}$ for $\mathfrak{m}$ maximal.

Corollary 9.3.1. *Let M be a finitely generated module over a local ring R. Let $\mathfrak{m}$ be its maximal ideal. Then $x_1, \ldots, x_n \in M$ generate M if and only if their image in $M \otimes_R (R/\mathfrak{m})$ generate it as an $R/\mathfrak{m}$ vector space.*

Proof. The forward direction is trivial. Conversely, suppose that the images of the x_i in $M \otimes_R (R/\mathfrak{m})$ generate it as an $R/\mathfrak{m}$ vector space. Let $R^{\oplus n} \longrightarrow M \longrightarrow Q \longrightarrow 0$ be exact, i.e. Q is the cokernel of the map $R^{\oplus n} \longrightarrow M$. We would like to show that $Q = 0$. Indeed, the surjection $M \longrightarrow Q$ yields a surjection $M/\mathfrak{m}M \longrightarrow Q/\mathfrak{m}Q$. As the x_i map to 0 in Q, their image maps to 0 in $Q/\mathfrak{m}Q$. As the x_i span $M/\mathfrak{m}M$ by assumption, their image spans $Q/\mathfrak{m}Q$, so $Q/\mathfrak{m}Q$ is 0, so as M is finitely generated Q is as well. Thus, we are done by Nakayama's lemma. □

10 Noetherian Rings

Definition 10.1. A ring R is called Noetherian if every increasing sequence of ideals terminates. Dually, we say a ring is Artinian if every descending sequence of ideals terminates.

The Noetherian condition is called the ascending chain condition (acc) for ideals, and the Artinian condition is called the descending chain condition (dcc) for ideals.

Lemma 10.1. *Let R be a ring. The following are equivalent.*

1. *R is noetherian*
2. *All ideals of R are finitely generated.*

Proof. 1) $\implies$ 2). Let I be an ideal of R. Suppose that I is not finitely generated. In particular, it is nonzero. Then let $x_1 \in I - 0$. As I is not finitely generated, $I \neq (x_1)$, so there exists $x_2 \in I - (x_1)$. Similarly, let $x_3 \in I - (x_1, x_2)$. Iterate this process to get a sequence $x_1, x_2, \ldots$. By construction, this ensures that $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$, but R is noetherian. 2) $\implies$ 1). Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of ideals. Then let $I = \bigcup_{n \geq 1} I_n$. One may check that this is an ideal. Then by assumption, it is finitely generated, so $I = (x_1, \ldots, x_n)$. Then there exists an $N \geq 1$ such that each $x_i \in I_N$. Then $I_N = I$, so the chain terminates at N. □

Examples. 1. Fields are both artinian and noetherian.

2. $\mathbb{Z}$ is noetherian but not artinian. Indeed, it is a PID and $1 < \infty$ so it is noetherian. Furthermore, we have the strictly descending sequence $(2) \supsetneq (4) \supsetneq (8) \supsetneq \ldots$, so $\mathbb{Z}$ is not artinian.

3. $k[x_1, x_2, \ldots]$ is not noetherian. Indeed, take $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$. However, as it is a domain, it is a subring of its quotient field, which is noetherian as it is a field. This shows that subrings of noetherian rings are not necessarily noetherian.

Lemma 10.2. *Any quotient of a noetherian ring is noetherian. The same goes for artinian rings.*

Proof. Correspondence. □

Definition 10.2. An R-module M is said to satisfy the acc for submodules if any increasing sequence of submodules terminates. Note that R is noetherian if and only if it satisfies acc as an R-module.

Lemma 10.3. *Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be an exact sequence of R-modules. Then B satisfies the acc if and only if A and C both do.*

Proof. Apply the five lemma to the chain of short exact sequences with chain maps defined by inclusion of the pullbacks and pushforwards of the chains. □

Theorem 10.4. *Let M be a finitely generated module over a noetherian ring R. Then every submodule of M is finitely generated and M satisfies the acc for submodules.*

Proof. Let $R^{\oplus n} \longrightarrow M$ a surjection. As these properties are preserved by quotients, it suffices to prove this for $R^{\oplus n}$. Indeed, we have the short exact sequence

$$0 \longrightarrow R \longrightarrow R^{\oplus n} \longrightarrow R^{\oplus n-1} \longrightarrow 0$$

So as R is noetherian, we are done by induction and the lemma. □

Lemma 10.5. *Any localization of a noetherian ring is noetherian.*

Proof. Let $S \subseteq R$ a multiplicative subset. We claim that all ideals $I \subseteq R[S^{-1}]$ can be written as $J \cdot R[S^{-1}]$ for some ideal $J \subseteq R$ an ideal. Indeed, let J be the preimage of I under the standard map $R \longrightarrow R[S^{-1}]$. Certainly, $J \cdot R[S^{-1}] \subseteq I$. Conversely, let $\frac{a}{s} \in I$. Then $\frac{a}{1} \in I$ so $a \in J$, so $\frac{a}{s} \in J \cdot R[S^{-1}]$. Hence, $J \cdot R[S^{-1}] = I$. Now, take some ideal $J = IR[S^{-1}]$ be an ideal. As R is noetherian, $I = (x_1, \ldots, x_n)$, so $J = (x_1, \ldots, x_n) \subseteq R[S^{-1}]$. Thus, $R[S^{-1}]$ is noetherian. □

Theorem 10.6 (Hilbert Basis Theorem)**.** *Let R be noetherian. Then $R[x]$ is noetherian.*

Proof. We show that ideals in $R[x]$ are finitely generated. Indeed, let $I \subseteq R[x]$ be an ideal. Let $I_j = \{a \in R : \exists\, f \in I$ of degree j with leading coefficient $a\}$. This is certainly an ideals in R, and we have $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, so as R is noetherian this terminates at, say, N. As R is noetherian, we can find a finite set of generators $\{f_{j,k}\}_{k=1}^{m_j}$ for each I_j. For each j, k there exists, by definition, a $g_{j,k} \in I$ of degree j with leading coefficient $f_{j,k}$. We claim that the $g_{j,k}$ for $j \leq N$ generate I. This is a finite set, so this will conclude the proof. Indeed, take $h \in I$. Let a be its leading coefficient, and let its degree be d. Suppose that $d \leq N$ Then $a = \sum_{i=1}^{m_d} b_j f_{d,j}$. Then $h - \sum_{i=1}^{m_d} b_j g_{d,j}$ has degree less than d, so we are done by induction. We must now only consider the case $d > N$. Indeed, then $a \in I_d = I_N$, so $a = \sum_{j=1}^{m_N} b_j f_{N,j}$. Then $h - x^{d-N} \sum_{j=1}^{m_N} b_j g_{N,j}$ has degree less than d, so we are done by induction. □

Remark. $k[x]$ is PID, but as proven in the homework, $k[x, y]$ has no upper bound on the number of generators needed per ideal. Specifically, we showed that the ideals $(x, y)^n$ cannot be generated by fewer than n elements. However, by the Hilbert Basis Theorem, this ring is nevertheless noetherian.

Corollary 10.6.1. *Finitely generated algebras over a noetherian ring are noetherian.*

11 Decomposition of Spec R into Irreducible Closed Subsets

Theorem 11.1. *Let R be a noetherian ring. Then $X = \operatorname{Spec} R$ is a finite union of irreducible closed subsets $X = X_1 \cup \cdots \cup X_n$ with no $X_i \subseteq X_j$ for $i \neq j$. Moreover, this decomposition is unique. We call these the irreducible components of X.*

Proof. Suppose that no such decomposition exists. Then in particular, X is nonempty and not irreducible. Hence, $X = X_1 \cup Y_1$, both of which are closed and neither are the whole of X. X_1 and Y_1 cannot both be written as a finite union of irreducibles as above, as otherwise X would have such a decomposition. Without loss of generality, say X_1 does not have such a decomposition. We repeat this process and deduce that $X_1 = X_2 \cup Y_2$ closed subsets, neither of which are the whole space, and X_2 having no such decomposition. Iterating this process, we get a strictly descending chain of irreducible closed subsets $X_1 \supsetneq X_2 \supsetneq X_3 \supsetneq \ldots$. This corresponds to a strictly increasing chain of ideals in R, contradicting R being noetherian. Thus, such a decomposition exists. The condition abotut $X_i \subseteq X_j$ can be achieved by deleting these repeats.
As for uniqueness, it suffices to show that for any radical ideal I, that if $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = I = \mathfrak{q}_1 \cap$

$\cdots \cap \mathfrak{q}_m$, the $\mathfrak{p}_i$ distinct prime ideals not containing each other. Similarly for the $\mathfrak{q}_j$. We have then that $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = \bigcap V(I) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$. We claim that each $\mathfrak{p} \in V(I)$ contains some $\mathfrak{p}_i$. If not, there exists some $x_i \in \mathfrak{p}_i - \mathfrak{p}$ for all i. Then $x = x_1 \dots x_n \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \subseteq \bigcap V(I) \subseteq \mathfrak{p}$, but $x \notin \mathfrak{p}$ by primality. In particular, each $\mathfrak{q}_j$ contains some $\mathfrak{p}_i$. Symmetrically, $\mathfrak{p}_i$ contains some $\mathfrak{q}_k$. Then $\mathfrak{q}_k \subseteq \mathfrak{p}_i \subseteq \mathfrak{q}_j$, so $k = j$ by assumption. Hence, each $\mathfrak{q}_j$ equals some $\mathfrak{p}_i$ and vice versa, proving the desired uniqueness. □

Theorem 11.2. *Let $I \subseteq R$ an ideal of a noetherian ring. Then there exists some $N \geq 1$ such that* $\mathrm{rad}(I)^N \subseteq I \subseteq \mathrm{rad}(I)$.

Proof. Of course, we need only show $\mathrm{rad}(I)^N \subseteq I$. As R is noetherian, $\mathrm{rad}(I) = (x_1, \dots, x_m)$. Let N be the max of the N_i such that $x_i^{N_i} \in I$. Let $a > Nm$ be an integer. Then Let $y_1, \dots, y_a$ be a not necessarily distinct generators of $\mathrm{rad}(I)$. Then by the pidgeonhole principle, some x_i^{N+1} divides $y_1 \dots y_a$. Then $y_1 \dots y_a \in I$, so $\mathrm{rad}(I)^a \subseteq I$, as any a-fold product of generators of $\mathrm{rad}(I)$ are in I. □

Lemma 11.3. *Let M be a nonzero module over a noetherian ring R. Then there exists a nonzero $x \in M$ such that* $\mathrm{Ann}_R(x)$ *is a prime ideal.*

Proof. Indeed, consider the set S of ideals of the form $\mathrm{Ann}_R(x)$ for $x \neq 0$. Indeed, as R is noetherian, this set has a maximal element. Call it $I = \mathrm{Ann}_R(x_0)$ for some $x_0 \neq 0$. We claim that this is prime. Indeed, $1 \notin I$ as $x_0 \neq 0$. Now let $ab \in I$. Suppose neither a nor b are in I. Then $ax_0, bx_0 \neq 0$ yet $abx_0 = 0$. Then $J = \mathrm{Ann}_R(ax_0) \in S$. Furthermore, $I \subseteq J$ as $rx_0 = 0$ implies that $rax_0 = 0$. Then $J = I$ by maximality. However, $b \in J$ as $abx_0 = 0$, yet $b \notin I$ as $bx_0 \neq 0$. Contradiction. □

Theorem 11.4. *Let M be a finitely generated module over a noetherian ring R. Then there is a finite sequence of submodules $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ such that each M_i/M_{i-1} is isomorphic to some $R/\mathfrak{p}_i$ for $\mathfrak{p}_i$ prime.*

Proof. If $M = 0$ we are done, so suppose otherwise. By the lemma, there exists some $x \neq 0$ such that $\mathfrak{p}_1 = \mathrm{Ann}_r(x)$ is prime. Let $M_1 = Rx$. Then $M_1/M_0 = M_1$ and $M_1 \cong R/\mathfrak{p}_1$ by the surjection $R \xrightarrow{\cdot x} M_1$. If $M = M_1$ we are done, so suppose otherwise. Then $M/M_1 \neq 0$, so there exists a submodule $P \subseteq M/M_1$ that is isomorphic to some $R/\mathfrak{p}_2$. Then let M_2 be the inverse image of P. This satisfies the desired property. Repeat this process. As M is finitely generated and R is noetherian, this process must terminate, so we get the desired filtration. □

12 Homological Algebra

Definition 12.1. A chain complex of R-modules is a sequence (indexed by $\mathbb{Z}$) of R-modules and R-linear maps between them

$$\dots \longrightarrow M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} M_{i-2} \longrightarrow \dots$$

such that $d^2 = 0$, i.e. $d_{i-1} \circ d_i = 0$ for all $i \in \mathbb{Z}$. Equivalently, that for all $i \in \mathbb{Z}$, that $\mathrm{im}(d_{i+1}) \subseteq \ker(d_i)$. We write this sequence as M_*.

Definition 12.2. For a chain complex M_*, we define the i^{th} homology $H_i(M_*) = \ker(d_i)/\operatorname{im}(d_{i+1})$. If each homology is 0, we say that the sequence is exact.

We would like to interpret the homology as a functor from the category of chain complexes to the category of R-modules. To do this, we must first define the morphisms in this category.

Definition 12.3. Let M_*, N_* be chain complexes. A chain map $f\colon M_* \longrightarrow N_*$ is a sequence of R-linear maps $f_i\colon M_i \longrightarrow N_i$ for all $i \in \mathbb{Z}$. such that the following diagram commutes.

$$\begin{array}{ccccccccc} \dots & \longrightarrow & M_i & \longrightarrow & M_{i-1} & \longrightarrow & M_{i-2} & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i-1}} & & \downarrow{\scriptstyle f_{i-2}} & & \\ \dots & \longrightarrow & M_i & \longrightarrow & M_{i-1} & \longrightarrow & M_{i-2} & \longrightarrow & \dots \end{array}$$

Omitting the indices, we write this condition as $df = fd$.

Indeed, for $i \in \mathbb{Z}$, we claim that H_i is a functor. Indeed, for $f\colon M_* \longrightarrow N_*$, we seek to define $H_i(f)\colon H_i(M_*) \longrightarrow H_i(N_*)$. Write the boundary maps of M_* as d and the boundary maps of N_* as e, so $ef = fd$. Indeed, we have a map

$$\ker(d_i) \xrightarrow{f_i} \ker(e_i) \longrightarrow \ker(e_i)/\operatorname{im}(e_{i+1})$$

which is well defined by the condition $ef = fd$. Indeed, this also says that the map vanishes on $\operatorname{im}(d_{i+1})$. This therefore induces a map $H_i(f)\colon H_i(M_*) \longrightarrow H_i(N_*)$ which one can check is functorial.
The category of chain complexes is actually a 2-category, so we will define the 2-morphisms.

Definition 12.4. Let $f, g\colon M_* \longrightarrow N_*$ be chain maps. A chain homotopy $F\colon f \longrightarrow g$ is a sequence of R-linear maps $F_i\colon M_i \longrightarrow N_{i+1}$ satisfying $dF + Fd = g - f$. We write $f \ g$ if there exists a homotopy $F\colon f \longrightarrow g$. One can check that this is an equivalence relation.

One can check that homology is well defined on homotopy classes of chain maps. This means that if $f \sim g$ then $H_i(f) = H_i(g)$.

Definition 12.5. A chain homotopy equivalence is a chain map $f\colon M_* \longrightarrow N_*$ such that there exists a chain map $g\colon N_* \longrightarrow M_*$ such that $fg \sim \mathrm{id}_{N_*}$ and $gf \sim \mathrm{id}_{M_*}$.

Then chain homotopy equivalence induces an isomorphism on homology groups, as functors preserve isomorphism and chain homotopy equivalences are isomorphisms up to homotopy.
We now define a homological notion that is essential to our future endeavors.

Definition 12.6. Let M be an R-module. A projective resolution is an exact sequence

$$\dots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

such that each P_i is projective.

Lemma 12.1. *Every R-module has a projective resolution.*

Proof. Indeed, we will show that a free resolution exists for any R-module M. We know that there exists an exact sequence

$$R^{\oplus I} \longrightarrow M \longrightarrow 0$$

Let K be the kernel of this map. Then we have

$$\begin{array}{ccccc} & & R^{\oplus I} & \longrightarrow & M \longrightarrow 0 \\ & & {\scriptstyle inc}\uparrow & & \\ R^{\oplus J} & \longrightarrow & K & \longrightarrow & 0 \end{array}$$

with exact rows. Then the sequence

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

by taking the composition is exact. Repeating this process yields a free, therefore projective, resolution. □

Lemma 12.2. *Any two projective resolutions are chain homotopy equivalent.*

Definition 12.7. Let $F\colon \mathbf{R-Mod} \longrightarrow \mathbf{S-Mod}$ be an additive, right exact functor. For example, $F = - \otimes_R S$. We define the left derived functors of F to be $F_i(M) = H_i(F(P_*))$ for some projective resolution P_* of M. This is well defined up to isomorphism by the above lemma.

Example. The essential example of a derived functor is Tor. We define $\mathrm{Tor}_i^R(-, N)$ to be the left derived functors of $- \otimes_R N$.

This is used to measure how much the tensor product fails to be exact. Recall that it is right exact, but not left exact in general. Indeed, using the snake lema one can show that any short exact sequence $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ induces a long exact sequence

$$\ldots \longrightarrow \mathrm{Tor}_2^R(M_3, N) \longrightarrow \mathrm{Tor}_1^R(M_1, N) \longrightarrow \mathrm{Tor}_1^R(M_2, N) \longrightarrow \mathrm{Tor}_1^R(M_3, N)$$

$$\longrightarrow M_1 \otimes_R N \longrightarrow M_2 \otimes_R N \longrightarrow M_3 \otimes_R N \longrightarrow 0$$

We can dually define the Ext functor by instead applying Hom to a projective resolution and taking the homology. These are not left derived functors due to the contravariance of Hom.

One can then use this construction to show that M is flat if and only of $\mathrm{Tor}_1^R(M, N) = 0$ for all R-modules N. We will use this to prove the ideal characterization of flatness mentioned previously.

Lemma 12.3. *An R-module M is flat if for all ideals I, tensoring with M preserves the injection $I \longrightarrow R$.*

Proof. Take an ideal I and consider the exact sequence $0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$. Tor induces an exact sequence.

$$\mathrm{Tor}_1^R(M,R) \longrightarrow \mathrm{Tor}_1^R(M,R/I) \longrightarrow M \otimes_R I \longrightarrow M \otimes_R R$$

As R is flat as an R-module, this becomes

$$0 \longrightarrow \mathrm{Tor}_1^R(M,R/I) \longrightarrow M \otimes_R I \longrightarrow M \otimes_R R$$

The rightmost arrow is injective by assumption, so $\mathrm{Tor}_1^R(M,R/I) = 0$ We want to prove that $\mathrm{Tor}_1^R(M,N) = 0$ for all R-modules N. We have done the case of $N = R/I$. We now consider the case when N is finitely generated. Let $N = \sum_{i=1}^n Rx_i$. Let $N_k = \sum_{i=1}^k Rx_i$. Then each N_k/N_{k-1} is cyclic, and is therefore isomorphic to some R/I, specifically we may take I to be the annihilator of the single generator of the cyclic module. Thus, by the previous work, $\mathrm{Tor}_1^R(M, N_k/N_{k-1}) = 0$ for all k. Then by induction and the long exact sequence of Tor, we get that $\mathrm{Tor}_1^R(M,N) = 0$.
Now, let N be any R-module. Then N is the direct limit of its finitely generated submodules. We know that the tensor product is cocontinuous and that direct limits factor through homology. Thus, $\mathrm{Tor}_1^R(M,R/I) = 0$, so M is flat. □

13 Integral Extensions

Definition 13.1. Let $A \subseteq B$ an extension of rings. We say $x \in B$ is integral over A is it is the root of a monic polynomial in A. Of course, for fields algebraic is equivalent to integral.

To gain motivation for this, consider the extension of rings $\mathbb{C}[x] \subseteq \mathbb{C}[x,y]$. Let $f \in \mathbb{C}[x,y]$. If f is monic over $\mathbb{C}[x]$, then $f = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x)$ for $a_i(x) \in \mathbb{C}[x]$. This tells us that after evaluating at any value of x, f has exactly n roots counting multiplicity. This is not the case whn $f = xy - 1$, for instance. Indeed, at $x = 0$ there are no roots and at $x = 1$ there is one root.

Example. Let K be a number field, i.e. a finite extension of $\mathbb{Q}$. We define $\mathcal{O}_K = \{x \in K : x \text{ is integral over } \mathbb{Z}\}$. This is called the ring of algebraic integers of K. We need to justify calling this a ring, which the following lemma will allow us to do.

Lemma 13.1. *Let $A \subseteq B$ an extension of rings. The following are equivalent.*

1. *$x \in B$ is integral over A.*
2. *The sub A-algebra of B generated by x is finite over A (finitely generated as an A-module). Call this algebra C.*
3. *The algebra C described above is contained in some finite A-algebra D.*
4. *There is a faithful (scalar multiplication is trivial if and only if the scalar is 0) C-module M that is finitely generated as an A-module.*

Proof. 1) $\implies$ 2) Let $x \in B$ integral over A. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for $a_i \in A$. Then $x^n \in A\{1, x, \ldots, x^{n-1}\} = C$, so C is a finite A-algebra.
2) $\implies$ 3) Take $D = C$.
3) $\implies$ 4) Let $M = D$. Then M is a C-module that is a finite A-algebra. Thus, it is a finitely generated A-module. Furthermore, as $1 \in D$, the module is faithful.
4) $\implies$ 1) Take C and M as given. Then $M = A\{m_1, \ldots, m_n\}$. Then as $x \in C$ and M is a C-module, each $xm_i \in M$. Then there exist a_{ij} for each i such that $xm_i = \sum_{i=1}^{n} a_{ij}m_j$. Let $Y = xI - (a_{ij})$ an $n \times n$ matrix with entries in C. Then let $m = (m_1, \ldots, m_n)$. The definition of the a_{ij} induce the equation $Ym = 0$. We have that $Y\text{adj}(Y) = \text{adj}(Y)Y = \det(Y)I$. Then $\det(Y)m = 0$. Thus, $\det(Y)$ kills the generators of M, so it kills all of M. Thus, $\det(Y) = 0$. $\det(Y)$ is a monic polynomial in x with coefficients in A, so x is indeed integral over A. $\square$

Definition 13.2. A ring homomorphism $A \longrightarrow B$ is called integral if B is integral over its image. Similarly, it is called finite if B is finite (i.e. a finitely generated module) over its image, and called finite type if B is finite time (i.e. a finitely generated algebra) over the its image.

Corollary 13.1.1. *A ring homomorphism $A \longrightarrow B$ is finite if and only if it is integral and of finite type.*

Proof. Finiteness certainly implies the other two properties. Conversely, suppose $A \longrightarrow B$ is finite type and integral. Assume without loss of generality that this map is the inclusion. Then $B = A[b_1,\ dots, b_n]$. By assumption, each b_i is integral over A. Then by condition 2 in the lemma, $A[b_1]$ is finite over A. The result then follows by induction, as b_2 is certainly integral over $A[b_1]$. $\square$

Lemma 13.2. *Let $A \subseteq B$ an extension of rings. Let C be the integral closure of A in B, i.e. all the elements of B that are integral over A, is a subrng of B.*

Proof. Indeed, let $x, y \in C$. Then x and y both satisfy monic polynomials over A. Let D be the A-algebra generated by $x^i y^j$ for $i \leq$ the degree of the monic polynomial x satisfies and $j \leq$ the degree of the monic polynomial y satisfies. Then D is a finite A-algebra so all of its elements are integral over A as the algebra they generate is contained in D. These elements include $x + y$, $x - y$, and xy. Thus, C is indeed a ring. $\square$

Definition 13.3. A domain R is called normal if it is integrally closed (i.e. equals its integral closure) in its quotient field.

Examples.
1. The ring of algebraic integers $\mathcal{O}_K$ is normal, as its quotient field is K and it is already defined as the integral closure of $\mathbb{Z}$ in K.
2. Any UFD is normal.

Lemma 13.3. *Let $A \subseteq B$ be integral. Then*

1. *For any ideal $I \subseteq B$, $A/(A \cap I) \longrightarrow B/I$ is integral.*
2. *For $A \subseteq A$ a multiplicative subset, $A[S^{-1}] \subseteq B[S^{-1}]$ is integral.*

Lemma 13.4. *Let $A \subseteq B$ an extension of rings. Let C be the integral closure of A in B. Then $C[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in $B[S^{-1}]$.*

Corollary 13.4.1. *Let A be a domain. The following are equivalent.*

1. *A is normal.*
2. *All localizations of A at prime ideals are normal.*
3. *All localizations of A at maximal ideals are normal.*

Which says that normality is a local property.

Proof. Note that $\mathrm{Frac}(A[S^{-1}]) = \mathrm{Frac}(A)$.
1) $\implies$ 2). Let A be normal. Let K be its quotient field. Let $\mathfrak{p} \subseteq A$ a prime ideal. Then the integral closure of $A_{\mathfrak{p}}$ in $\mathrm{Frac}(A_{\mathfrak{p}}) = K$ is $A_{\mathfrak{p}}$ by the lemma.
2) $\implies$ 3). Clear.
3) $\implies$ 1). Let C be the integral closure of A in K. We want to show that $A = C$. Equivalently, we want to show that the inclusion map $A \longrightarrow C$ is surjective. We know that a map being surjective is a local property. Furthermore, by assumption, each inclusion $A_{\mathfrak{m}} \longrightarrow C_{\mathfrak{m}}$ is surjective, as these domains are normal and by the lemma $C_{\mathfrak{m}}$ is the integral closure of $A_{\mathfrak{m}}$ in K. Hence, the inclusion $A \longrightarrow C$ is surjective as desired. □

Example. Let K be a umber field. As discussed above, $\mathcal{O}_K$ is normal, but is not in general a UFD. Indeed, one may show that the localization of $\mathcal{O}_K$ at any maximal ideal is a discrete valuation ring, hence a PID, hence a UFD, hence normal.

14 Behavior of Prime Ideals under Integral Extensions

Lemma 14.1. *Let $A \subseteq B$ integral. Then we have the induced map $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ via $\mathfrak{q} \mapsto \mathfrak{q} \cap A$. We claim that $\mathfrak{q}$ is maximal if and only if $\mathfrak{q} \cap A$ is maximal. Observe that this fails when the extension is not integral. For example, consider the inclusion $\mathbb{C} \subseteq \mathbb{C}[x]$. The associated map on spectra takes $0 \subseteq \mathbb{C}[x] \mapsto 0 \subseteq \mathbb{C}$, i.e. a nonmaximal ideal maps to a maximal ideal.*

Proof. By a lemma in the previous section, $B/\mathfrak{q}$ is integral over $A/\mathfrak{q} \cap A$. It therefore suffices to show that for $A \subseteq B$ an integral extension of domains, that B is a field if and only if A is. Indeed, let A be a field. Let $y \in B - 0$. Then as the extension is integral, we have $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$ for $a_i \in A$. Let n be minimal. Then $a_0 \neq 0$, as otherwise we may cancel out y as we are in a domain. We have then that $y(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1) = -a_0 \in A - 0 \in A^\times$, so $y \in B^\times$, so B is a field.
Conversely, let B be a field. Let $x \in A - 0$. We have that $x^{-1} \in B$ exists. We claim that it's in A. Indeed, we have that it satisfies some $x^{-n} + a_{n-1}x^{-(n-1)} + \cdots + a_0 = 0$, $a_i \in A$. We multiply this equation by x^{n-1} to yield $x^{-1} = -(a_{n-1} + a_{n-2}x + \cdots + a_)x^{n-1}) \in A$, so A is a field. □

We have the following results about the associated map on spectra.

1. If $A \mapsto B$ is onto, then $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is the inclusion of a closed subset.
2. The map $A \longrightarrow A[S^{-1}]$ induces the map $\mathrm{Spec}(A[S^{-1}]) \longrightarrow \mathrm{Spec}(A)$ is injective.

We would like to investigate what happens in the case of the map being finite or integral.

Definition 14.1. An affine scheme X is the spectrum of some ring. We write $\mathcal{O}(X)$ for this ring. This is called the ring of regular functions on X. A morphism of affine schemes $X \longrightarrow Y$ is the spectral map of a ring homomorphism $\mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$. We say morphism of affine schemes is finite, finite type, or integral if the associated ring map is finite, finite type, or integral respectively. Of course, this says that we can view the category of affine schemes as the opposite category of the category of commutative rings.

Lemma 14.2. *Let $A \subseteq B$ integral. Let $\mathfrak{q} \subseteq \mathfrak{q}' \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. As $A \subseteq B$ is integral, $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$ is integral. This is a slight abuse of notation, as $\mathfrak{p}$ is not necessarily a prime ideal (or an ideal) of B. We write $B_{\mathfrak{p}} = B[(A - \mathfrak{p})^{-1}]$. let $\mathfrak{m}$ be the maximal ideal of the lcoal ring $A_{\mathfrak{p}}$. Then $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$. Let $\mathfrak{n} = \mathfrak{q}B_{\mathfrak{p}}$, $\mathfrak{n}' = \mathfrak{q}'B_{\mathfrak{p}}$. Then as $\mathfrak{q} \subseteq \mathfrak{q}'$, $\mathfrak{n} \subseteq \mathfrak{n}'$. We claim that $\mathfrak{n} \cap A_{\mathfrak{p}} = \mathfrak{n}' \cap A_{\mathfrak{p}} = \mathfrak{m}$. This holds as localization commutes with pulling back prime ideals by correspondence. Then as these pull back to a maximal ideal, $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal, so as $\mathfrak{n} \subseteq \mathfrak{n}'$, they are equal. Thus, by correspondence, $\mathfrak{q} = \mathfrak{q}'$. □

Theorem 14.3. *Let $A \subseteq B$ integral. Then the map $\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$ is onto, i.e. all prime ideal $\mathfrak{p} \subseteq A$ are of the form $\mathfrak{q} \cap A$ for some prime ideal $\mathfrak{q} \subseteq B$.*
This need not hold for non-integral extensions. Indeed, consider $k[t] \subseteq k[t, t^{-1}]$. As discussed previously, the spectral map of a localization is injective, so the map $\mathrm{Spec}(k[t, t^{-1}]) \longrightarrow \mathrm{Spec}(k[t])$, which we view as the inclusion of the open subset $\mathrm{Spec}(k[t]) - \{0\}$. We may also view $k[t, t^{-1}]$ as $k[x, y]/(xy - 1)$, so the map looks like

Proof. Let $\mathfrak{p} \subseteq A$ be a prime ideal. As $A \subseteq B$ is integral, $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$ is also integral. By exactness of localization, we have the commutative diagram

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

$A_\mathfrak{p}$ is local, therefore it is nonzero so $B_\mathfrak{p}$ is nonzero. Then let $\mathfrak{n} \subseteq B_\mathfrak{p}$ be maximal. its pullback to $A_\mathfrak{p}$ is maximal, so as $A_\mathfrak{p}$ is local it equals its maximal ideal $\mathfrak{m} = \mathfrak{n} \cap A_\mathfrak{p}$. Now, let $\mathfrak{q}$ be the pullback of $\mathfrak{n}$ along $B \longrightarrow B_\mathfrak{p}$. Then the pullback of $\mathfrak{q}$ along $A \longrightarrow B$ is $\mathfrak{p}$, as can be seen by applying the Spec functor to the above commutative diagram. Thus, the map $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is onto. □

15 The Noether Normalization Lemma and the Nullstellensätze

Lemma 15.1. *Let k be a field. Let $f \in k[x_1, \ldots, x_n] - 0$. Then there exists a k-algebra homomorphism $k[x_1, \ldots, x_n] \longrightarrow k[y_1, \ldots, y_n]$ such that f maps to a nonzero constant times a monic polynomial in y_n, i.e. $f = cy_n^d +$ (terms of lower n-degree). Geometrically, this means that given any hypersurface $\{f = 0\} \subseteq \mathbb{A}_k^n$ we can change coordinates such that $\{f = 0\} \longrightarrow \mathbb{A}_k^n \longrightarrow \mathbb{A}_k^{n-1}$ is a finite morphism. For example, take $f = x_1x_2 - 1 \in k[x_1, x_2]$. The closed subset $\{f = 0\} \subseteq \mathbb{A}_k^2$ looks like*

on which we can apply the change of coordinates $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, which looks like rotation. Indeed, in $k[y_1, y_2]$, $f = y_1^2 - y_2^2 - 1$. The closed subset $\{f = 0\} \subseteq \mathbb{A}_k^2$ looks like

Proof. Let $f \in k[x_1, \ldots, x_n] - 0$. We write $f = \sum a_I x^I$, where I ranges over tuples $(i_1, \ldots, i_n) \in \mathbb{N}^n$ and $a_I = a_{i_1,\ldots,i_n}$ and $x^I = x^{i_1} \ldots x^{i_n}$. Of course, we require all but finitely many a_I to be 0. Let $(i_1, \ldots, i_n)$ be a maximal (under the lexicographic ordering) such that $a_I \neq 0$. Let $m_1 >> m_2 >> \cdots >> m_{n-1} >> 1$. Then $f(y_1 + y_n^{m_1}, \ldots, y_{n-1} + y_n^{m_{n-1}}, y_n) = a_{i_1,\ldots,i_n} y_n^{m_1 i_1 + m_2 i_2 + \cdots + m_{n-1} i_{n-1} + i_n} +$(lower total degree terms). One can see this by seeing that in expanding out $f(y_1 + y_n^{m_1}, \ldots, y_{n-1} + y_n^{m_{n-1}}, y_n)$, the i_1 term is given more weight via m_1 being large relative to the other m_k. One can check that this change of variables is an isomorphism and that f satisfies the desired property in the image. □

Theorem 15.2 (Noether Normalization Lemma)**.** *Let $R \neq 0$ be a finitely generated algebra over a field k. Then there exists $n \geq 0$ such that there exists a finite inclusion $k[x_1, \ldots, x_n] \longrightarrow R$.*

Proof. We have a surjection $k[x_1, \ldots, x_N] \longrightarrow R$ by assumption. Let N be minimal. If $N = 0$, then $k \longrightarrow R$ is a surjection, so as $R \neq 0$, $R = k$ and we are done. Else, let I be the kernel of the map. Again, if it's 0 then we are done. Suppose not, then let $f \in I - 0$. By the lemma, we may suppose that f is a nonzero constant time a monic polynomial in x_N. That monic polynomial itself is in I as I is an ideal. This allows us to kill higher powers of x_N, so there is a finite map $k[x_1, \ldots, x_{N-1}] \longrightarrow R$. Call the image of this map S. Then by induction, S is finite over some $k[x_1, \ldots, x_n] \subseteq S$, so R is. □

Geometrically, this says that for X an affine scheme of finite type over k, we get an $n \geq 0$ and a finite surjection $X \longrightarrow \mathbb{A}^n_k$. We have the following picture

Corollary 15.2.1 (Hilbert's Nullstellensatz, weak form)**.** *Let R be an algebra of finite type over a field k such that R is a field. Then R is finite over k.*

Proof. By the Noether normalization lemma, there exists a finite inclusion $k[x_1, \ldots, x_n] \longrightarrow R$. As R is a field, 0 is a maximal ideal of R so its pullback along this map is maximal. Of course, this is just the kernel of this map, which is 0. Thus, $k[x_1, \ldots, x_n]$ is a field, so $n = 0$ and we are done. □

Corollary 15.2.2 (Hilbert's Nullstellensatz, another form)**.** *Let k be an algebraically closed field. We know that even without the algebraically closed assumption, there is an inclusion $k^n \subseteq \mathbb{A}^n_k$ via $(a_1, \ldots, a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n)$, which is a maximal ideal, hence a closed point. With this additional assumption, we have that all maximal ideals (hence all closed points) are of this form.*

Proof. Let $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ maximal. Then $k[x_1, \ldots x_n]/\mathfrak{m}$ is a field that is a k-algebra of finite type. Then by the weak Nullstellensatz, it's finite over k. As k is algebraically closed, it equals k. Thus, we have a surjection $f \colon k[x_1, \ldots, x_n] \longrightarrow k$ with kernel $\mathfrak{m}$. By freeness, f is toally and uniquely determined by the choice of $c_i = f(x_i)$. Indeed, f is simply evaluation at $(c_1, \ldots, c_n)$. Thus, we have $(x_1 - c_1, \ldots x_n - c_n)$, which is the ideal of polynomials vanishing at $(c_1, \ldots, c_n)$, is contained in the kernel $\mathfrak{m}$. As these are both maximal, $\mathfrak{m} = (x_1 - c_1, \ldots, x_n - c_n)$. □

Remark. As discussed, for k not algebraically closed we still have the inclusion $k^n \subseteq \mathbb{A}^n_k$, but it does not necessarily consist of all closed points. Indeed, for $k = \mathbb{R}$, the maximal ideal $(x^2 + 1)$ is not of this form. In fact, the converse holds as well, i.e. if k is not algebraically closed then there exists a maximal ideal not of this form for some n. Indeed, if k is not algebraically closed then there is a proper finite field extension K/k. Then K is, in particular a finite type k-algebra, so we have a surjection $k[x_1, \ldots, x_n] \longrightarrow K$. Its kernel is then a maximal ideal, and cannot be of this form, as $k[x_1, \ldots, x_n]/(x_1 - c_1, \ldots, x_1 - c_n) = k \neq K$.

Definition 15.1. The Jacobson radical of a ring R is the intersection of all maximal ideals of R. We write this as $J(R)$

Remark. We always have $\mathrm{nil}(R) \subseteq J(R)$. However, the converse need not hold. Indeed, take the local ring $R = \mathbb{Z}_{(2)}$. Then as R is a domain, its nilradical is trivial, yet its Jacobson radical is the unique maximal ideal $(2)\mathbb{Z}_{(2)}$, which is nonzero.

Lemma 15.3. *Let R be an algebra of finite type over a field k. Then $J(R) = \mathrm{nil}(R)$.*

Proof. As discussed, $\mathrm{nil}(R \subseteq J(R)$. Conversely, let $f \in J(R)$. Take a prime ideal $\mathfrak{p}$. We would like to show that $f = 0$ in $R/\mathfrak{p}$. By correspondence, $f \in J(R/\mathfrak{p})$. Furthermore, $R/\mathfrak{p}$ is an algebra of finite type over k. Then it suffices to show that the Jacobson radical of a domain of finite type over a field is trivial. Let R be such a domain. Let $f \in J(R)$. If $f \neq 0$ then $R[1/f]$ is a domain of finite type over k. Then $R[1/f]$ contains a maximal ideal $\mathfrak{m}$. By the weak Nullstellensatz, $R[1/f]/\mathfrak{m}$ is finite over k. Consider $\mathfrak{n} = \ker(R \longrightarrow R[1/f]/\mathfrak{m})$. The image of this map is a subring of a field, so it is therefore a domain. It is also a finite k-algebra, so it is a field. Thus, $\mathfrak{n}$ is maximal. Then $f \notin \mathfrak{n}$ but $f \in J(R \subseteq \mathfrak{n}$, a contradiction. □

Theorem 15.4 (Hilbert's Nullstellensatz, strong form)**.** *Let k be an algebraically closed field. For $I \subseteq k[x_1, \ldots, x_n]$ an ideal. Let $Z(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0$ for all $f \in I\}$, called the zero set of I. Then the ideal of polynomials vanishing on $Z(I)$ is $\mathrm{rad}(I)$. Note that this can fail for non-algebraically closed fields. Indeed, take $k = \mathbb{R}$, $I = (x^2 + 1) \subseteq \mathbb{R}[x]$. Then $Z(I) = \emptyset$, so the ideal of polynomials vanishing on $Z(I)$ is $\mathbb{R}[x]$, but as $x^2 + 1$ is irreducible, $(x^2 + 1)$ is maximal, hence prime, hence radical and not equal to $\mathbb{R}[x]$.*

Proof. Let J be the ideal of polynomials vanishing on $Z(I)$. Certainly, $I \subseteq J$. Furthermore, if $f^r \in J$ then $f \in J$ as we are in a domain. Hence, J is radical and $\mathrm{rad}(I) \subseteq J$. Let $R = k[x_1, \ldots, x_n]/\mathrm{rad}(I)$. This is an algebra of finite type over k, so $J(R) = \mathrm{nil}(R) = 0$. Let $f \notin \mathrm{rad}(I)$. Then f is nonzero in $R/\mathrm{rad}(I)$, so as $J(R) = 0$ there is some maximal ideal $\mathfrak{m} \subseteq R$ that does not contain f. This pulls back to a maximal ideal in $k[x_1, \ldots, x_n]$, which is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ by the Nullstellensatz. Furthermore, this maximal ideal contains $\mathrm{rad}(I)$. Let $a = (a_1, \ldots, a_n)$. As $f \notin \mathrm{rad}(I)$, $f(a) \neq 0$. Furthermore, as $\mathrm{rad}(I) \subseteq \mathfrak{m}$, $a \in Z(\mathrm{rad}(I)) = Z(I)$. Thus, $f \notin J$ as desired. □

16 Artinian Rings

Recall that a ring is artinian if it satisfies the dcc for ideals, i.e all descending sequences of ideals terminate. This is dual to the notion of a noetherian ring, which satisfies the acc. Surprisingly, one can show that all artinian rings are noetherian.

Lemma 16.1. *In an artinian ring, all prime ideals are maximal.*

Proof. It suffices to show that artinian domains are fields. Indeed, let R be an artinian domain and let $x \in R - 0$. Then consider the descending sequence of ideals $(x) \supseteq (x^2) \supseteq (x^3) \supseteq \dots$. As R is artinian, this must terminate, so some $(x^n) = (x^{n+1})$. In particular, $x^n \in (x^{n+1})$, so $x^n = yx^{n+1}$, As R is a domain and $x \neq 0$, $1 = xy$ so $x \in R^\times$. Then R is a field. □

Lemma 16.2. *Artinian rings have finitely many maximal ideals.*

Proof. Suppose there are distinct maximal ideals $\mathfrak{m}_k$ for $k \geq 1$. Then we have the descending sequence $\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \dots$. Then we get a (strictly) ascending sequence $V(\mathfrak{m}_1) \subseteq V(\mathfrak{m}_1 \cap \mathfrak{m}_2) \subseteq \dots$, which is $V(\mathfrak{m}_1) \subseteq V(\mathfrak{m}_1) \cup V(\mathfrak{m}_2) \subseteq \dots$, which is $\{\mathfrak{m}_1\} \subseteq \{\mathfrak{m}_1, \mathfrak{m}_2\} \subseteq \dots$. However, this contradicts R being artinian, as maximal ideals are radical. □

These two lemmas combine to tell us that the spectrum of an artinian ring is a finite discrete space.

Definition 16.1. The length of a strictly increasing chain of prime ideals $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_r$ is r. The (Krull) dimension of a ring R is the supremum of the lengths of strictly increasing chains of prime ideals.

We see immediately that a ring has dimension 0 if and only if all prime ideals are maximal. Then the lemma says that artinian rings have dimension 0. The converse is not true. For example, let $R = k[x_1, x_2, \dots]/(x_i^2 : i \geq 1)$. Take a prime ideal $\mathfrak{p} \subseteq R$. We have $0 = x_i^2 \in \mathfrak{p}$, so $x_i \in \mathfrak{p}$. Thus, $\mathfrak{p} = (x_1, x_2, \dots)$, which is maximal. However, we will show that artinian = noetherian + dimension 0.

Examples. 1. a PID has dimension 1

2. $k[x_1, x_2, \dots]$ has infinite dimension.

3. $\dim(0) = -\infty$ as $\sup(\emptyset) = \infty$. Furthermore, $\dim(R) = -\infty$ if and only if $R = 0$.

4. What is $\dim(k[x_1, \dots, x_n])$? We have the chain $0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \dots \subsetneq (x_1, x_2, \dots, x_n)$, which has length n, so $\dim(k[x_1, \dots, x_n]) \geq n$. It turns out that $\dim(k[x_1, \dots, x_n]) = n$.

Definition 16.2. For a topological space X, define $\dim(X)$ to be the supremum of lengths of strictly increasing chains of irreducible closed subsets of X.

Of course, the dimension of $\mathrm{Spec}(R)$ is equal to the dimension of R by the correspondence between irreducible closed subsets of $\mathrm{Spec}(R)$ and R.

We now proceed in the proof that artinian = noetherian + dimension 0.

Lemma 16.3. *Let R be an artinian ring. Then $\mathrm{nil}(R)$ is nilpotent, i.e. there exists an $n \geq 0$ such that $\mathrm{nil}(R)^n = 0$. Recall that for a noetherian ring, we have that $\mathrm{rad}(I)^n \subseteq I \subseteq \mathrm{rad}(I)$.*

Proof. Consider the descending chain $\text{nil}(R) \supseteq \text{nil}(R)^2 \supseteq \dots$. This must terminate, so there is some $m \geq 0$ such that $\text{nil}(R)^m = \text{nil}(R)^n$ for all $n \geq m$. Now let $I = \text{nil}(R)^m$. We claim that $I = 0$. Suppose otherwise. Let $S = \{J \subseteq R \text{ an ideal} : IJ \neq 0\}$. This is nonempty as $R \in S$ by assumption. As R is artinian, there is a least element of S, which we call J. Furthermore, as $IJ \neq 0$, there exists an $x \in J$ such that $xI \neq 0$. Hence, $(x) \subseteq J$ is in S, so by minimality, $J = (x)$. We can reduce this further. Indeed, $(xI)I = xI^2 = xI \neq 0$, so $xI = (x) = J$. Then there exists a $y \in I$ such that $xy = x$. Then we get $x = xy = xy^2 = xy^3 = \dots$. However, as $y \in I \subseteq \text{nil}(R)$, some $y^n = 0$, so $x = xy^n = 0$, a contradiction. □

Theorem 16.4. *A ring is artinian if and only if it is noetherian and dimension 0.*

Proof. Let R be artinian. We know that $\dim(R) = 0$, so it suffices to show that R is noetherian. Indeed, let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the maximal ideals of R. These are all the prime ideals, so $\text{nil}(R) = \bigcap_{i=1}^n \mathfrak{m}_i$. Hence, $\text{nil}(R) \supseteq \mathfrak{m}_1 \dots \mathfrak{m}_n$. By the lemma, there exists a $b \geq 1$ such that $\text{nil}(R)^b = 0$. Thus, $(\mathfrak{m}_1 \dots \mathfrak{m}_n)^b$. Then $\mathfrak{m}_1^b \dots \mathfrak{m}_n^b = 0$. By relabeling, we have the sequence $R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \dots \supseteq \mathfrak{m}_1 \dots \mathfrak{m}_n = 0$ of maximal ideals.
Note that by linear algebra, for a vector space V over a field k, the acc, dcc, and finite dimensionality are all equivalent. Furthermore, given an R-module M, the R-submodules of $M/\mathfrak{m}M$ are the same as the $R/\mathfrak{m}$ submodules of $M/\mathfrak{m}M$. As submodules and quotients of modules over an artinian ring are artinian, the successive quotients of the sequence described above are artinian R-modules. Thus, they are artinian $R/\mathfrak{m}$ modules for any maximal ideal $\mathfrak{m}$. Thus, they are also noetherian R-modules, so by induction R is a noetherian R-module, hence a noetherian ring. The converse is similar. □

Definition 16.3. A dedekind domain is a noetherian normal domain of dimension 1.

Examples. 1. PIDs are dedekind domains.

2. $\mathcal{O}_K$ is a dedekind domain for any number field K.

17 Discrete Valuation Rings

Definition 17.1. Let K be a field. A discrete valuation on K is a surjection $v \colon K \longrightarrow \mathbb{Z} \cup \{\infty\}$ satisfying the following:

1. $v(x) = \infty$ if and only if $x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq min\{v(x), v(y)\}$

We call $\{x \in K : v(x) \geq 0\}$ the discrete valuation ring (DVR) associated to (K, v).

The idea is that v measure the degree of vanishing of an element of K. We think of an element of K as small if its valuation is large.

1. $K = k(x)$. Any nonzero element of K can be written uniquely as $x^m \frac{f}{g}$ with $f(0) \neq 0 \neq g(0)$. We define the valuation of this to be m, and the valuation of 0 to be 0. Indeed, this measures the order vanishing of a rational function at 0.

2. $K = \mathbb{Q}$, $p \in \mathbb{Z}$ a prime. As $\mathbb{Z}$ is a UFD, any nonzero element of $\mathbb{Z}$ can be written uniqely as $p^a m$ with $p \nmid m$. Then any nonzero element of $\mathbb{Q}$ can be written uniquely as $p^m \frac{a}{b}$ with $p \nmid a$. We define the valuation v_p of this to be m, and the valuation of 0 to be 0. This measures the "p-ness" of an element. This can be easily generalized to any irreducible element of a PID.

Lemma 17.1. *The associated DVR of a valuation (K, v) is a local ring with maximal ideal $\mathfrak{m} = \{x \in K : x > 0\}$*

Proof. One can easily check that the associated DVR R is a subring of K. We show that $\mathfrak{m} = R - R^\times$. Indeed, $v(1) = v(1 \cdot 1) = v(1) + v(1)$, so $v(1) = 0$, Furthermore, if $xy = 1$ in R then $0 = v(1) = v(xy) = v(x) + v(y)$, so as $v(x), v(y) \geq 0$, $v(x) = v(y) = 0$. Thus, $\mathfrak{m} \subseteq R - R^\times$. Conversely, let $v(x) = 0$. Then as $x^{-1} \in K$ exists, we have $v(x^{-1}) = -v(x)$ as it is a group homomorphism of $K^\times$. Then $v(x) = v(x^{-1}) = 0$, so $x^{-1} \in R$. Thus, $x \in R^\times$, so $\mathfrak{m} = R - R^\times$ as desired. □

Furthermore, we can describe all the ideals of the associated DVR of a discrete valuation R. Indeed, for $I \neq 0$, let n be the smallest valuation of elements in I. Then by surjectivity of the valuation, there exists an element $x \in R$ with valuation n. Furthermore, any $y \in I$ satisfies $v(y) \geq n$. Thus, $v\left(\frac{y}{x}\right) = v(y) - v(x) \geq 0$, so $\frac{y}{x} \in R$. Then $y \in (x)$, so $I = (x)$. In particular, all DVRs are PIDs. We can in fact go further. It's clear now that the unique maximal ideal $\mathfrak{m}$ is equal to any (x) with $v(x) = 1$. We claim that all nonzero ideals of R are of the form (x^a). Indeed, one can show that $v(x) = v(y)$ if and only if x and y are associate. Then for $0 \neq I = (y)$, we have $y \approx x^n$, so $I = (x^n) = \mathfrak{m}^n$. This furthermore implies that $\dim(R) = 1$.

Remark. If a ring R can be viewed as the associated DVR, there is a unique way to do so. Indeed, R must be a domain so take $K = \mathrm{Frac}(R)$. Then for $x \in R$, $v(x)$ is forced to be the largest $a \in \mathbb{N}$ such that $x \in \mathfrak{m}^a$. This says that being a DVR is a property of the ring itself.

Theorem 17.2. *Let R be a noetherian local domain of dimension 1. Let $\mathfrak{m}$ be its maximal ideal, $k = R/\mathfrak{m}$ its residue field. The following are equivalent.*

1. *R is DVR*
2. *R is normal*
3. *$\mathfrak{m}$ is principal*
4. *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$*
5. *Every nonzero ideal in R is a power of $\mathfrak{m}$*
6. *There exists an $x \in R$ such that every nonzero ideal of R equals some (x^a)*

Proof. We first prove some general properties of R.
Firstly, the spectrum of R is a closed point and its generic point as it has a unique maximal ideal and it having dimension 1 says that prime ideals are 0 or maximal.
Furthermore, for any nonzero proper ideal I, $\mathrm{rad}(I) = \mathfrak{m}$. Then as R is noetherian, there

exists an n such that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.
1) $\implies$ 2). DVRs are PIDs, hence UFDs, hence normal.
2) $\implies$ 3). Let $a \neq 0$ in $\mathfrak{m}$. Then as said above, $\mathfrak{m}^n \subseteq (a) \subseteq \mathfrak{m}$. let n be minimal. Then $\mathfrak{m}^{n-1} \subsetneq (a)$. let $b \in \mathfrak{m}^{n-1} - (a)$. Then $x = \frac{a}{b} \in K = \text{Frac}(R)$. Then $x^{-1} \notin R$ as if it were then $\frac{b}{a} \in R$, which would imply that $b \in (a)$, a contradiction. Thus, as R is normal, x^{-1} is not integral over R. Furthermore, if $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$ then we would have $x^{-a}\mathfrak{m} \subseteq \mathfrak{m}$ for all $a \geq 1$. Then $\mathfrak{m}$ is a faithful $R[x^{-1}]$-module that is finitely generated as an R-module, as R is noetherian. Thus, by a previous characterization of integrability, this says that x^{-1} is integral, a contradiction. Hence, $x^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$. However, $x^{-1}\mathfrak{m} \subseteq R$ as $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$. Thus, $x^{-1}\mathfrak{m}$ contains a unit of R, as $\mathfrak{m} = R - R^\times$. Thus, $x^{-1}\mathfrak{m} = R$ so $\mathfrak{m} = (x)$.
3) $\implies$ 4). Let $\mathfrak{m} = (x)$. Then x spans $\mathfrak{m}/\mathfrak{m}^2$ as a k vector space, so its k dimension is at most 1. If $\mathfrak{m}/\mathfrak{m}^2 = 0$ then by Nakayama's lemma, we would have $\mathfrak{m} = 0$. However, $\dim(R) = 1$, so R is not a field, so this is impossible.
4) $\implies$ 5). Let $0 \neq \subsetneq R$ an ideal. We have that $\mathfrak{m}^n \subseteq I$ for some n. Let r be minimal such that I contains an element a of $\mathfrak{m}^r - \mathfrak{m}^{r-1}$. Clearly, $r \leq n$. Furthermore, as $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, $\dim_k(\mathfrak{m}^r/\mathfrak{m}^{r+1}) = 1$. Indeed, $\{a\}$ is a basis for this, so $(a) = \mathfrak{m}^r$ by Nakayama's lemma. Then $I = \mathfrak{m}^r$ by minimality.
5) $\implies$ 6). Clear as we can repeat the argument in 4) $\implies$ 5) to show that $\mathfrak{m}$ is principal.
6) $\implies$ 1). For $x \in R$ define

$$v(x) = \begin{cases} r & x \in \mathfrak{m}^r - \mathfrak{m}^{r+1} \\ 0 & x = 0 \end{cases}$$

and check that this works. □

Definition 17.2. Let $\mathfrak{p} \subseteq R$ be a prime ideal. We define its codimension $\text{codim}(\mathfrak{p})$ to be the supremum of the lengths of strictly increasing chains of prime ideals contained in $\mathfrak{p}$.

Lemma 17.3. $\text{codim}(R_\mathfrak{p}) = \text{codim}(\mathfrak{p})$

Proof. Correspondence. □

Examples. 1. Let R be a domain. Then $\text{codim}(0) = \dim(R_{(0)}) = \dim(\text{Frac}(R)) = 0$.

2. Let R be a noetherian normal domain, $\mathfrak{p}$ be a codimension 1 prime ideal. Then $R_\mathfrak{p}$ has dimension 1 and is therefore a noetherian normal local domain of dimension 1, which is a DVR by the theorem.

3. Let R be a UFD, $f \in R$ irreducible. Then (f) has codimension 1. Indeed, we have $0 \subsetneq (f)$ so $\text{codim}((f)) \geq 1$. Suppose we have $0 \subsetneq \mathfrak{q} \subsetneq (f)$. Then let $g \in \mathfrak{q} - 0$. We then have $g = fh$. As $f \notin \mathfrak{q}$, we have $h \in q$. Then $\mathfrak{q} = f\mathfrak{q}$, so $\mathfrak{q} = f\mathfrak{q} = f^2\mathfrak{q} = \ldots$. Then as $g \in \mathfrak{q}$, $f^r \mid g$ for all $r \geq 0$, which is impossible in a UFD unless $g = 0$.

18 Dimension of a Polynomial Ring

The goal of this section is to show that the dimension of a polynomial ring in n variables over a field has dimension n. The key idea is that an integral extension of rings preserves dimension. This will yield our induction.

Lemma 18.1. *Let $A \subseteq B$ be an integral exntension. Then* $\dim(A) = \dim(B)$.

Proof. We have that the map $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is onto. Any chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ can be lifted, by surjectivity, to $\mathfrak{q}_i \subseteq B$ prime. These are distinct as they map to distinct elements in $\mathrm{Spec}(A)$. Thus, this is a chain of length n in B, so $\dim(B) \geq n$. Thus, $\dim(A) \leq \dim(B)$. If $\dim(A) = \infty$ we are done. Suppose then that $\dim(A) = n$.
Suppose that there exists a chain of length $n+1$ $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_{n+1}$ of primes in B. Let $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. By a previous result, distinct nested prime ideals map to distinct primes in an integral extension. Thus, this becomes a chain of length $n+1$ in A, a contradiction. □

Theorem 18.2. $\dim(k[x_1, \ldots, x_n]) = n$

Proof. The base case of $n = 0$ is easy, as fields have dimension 0.
We know that $\dim(k[x_1, \ldots, x_n]) \geq n$. On the other hand, let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain of primes in $k[x_1, \ldots, x_n]$. We then want $r \leq n$. We have that $\mathfrak{p}_1 \neq 0$, so let $f \in \mathfrak{p}_1 - 0$. We may assume without loss of generality that f is a nonzero constant times a monic polynomial in x_n. Then this monic polynomial is in $\mathfrak{p}_1$. This creates a relation in $k[x_1, \ldots, x_n]/\mathfrak{p}_1$ that allows us to kill higher degree terms. Indeed, this tells us that $k[x_1, \ldots, x_n]/\mathfrak{p}_1$ is finite over $k[x_1, \ldots, x_{n-1}]$. By the Noether normalization lemma, there is some s such that $k[x_1, \ldots, x_s] \subseteq k[x_1, \ldots, x_n]/\mathfrak{p}_1$ is a finite (hence integral) extension of rings. The above tells us that we can take $s \leq n-1$. By induction, $\dim(k[x_1, \ldots, x_s]) = s$, so by the lemma, $\dim(k[x_1, \ldots, x_n]/\mathfrak{p}_1) = s$. Then by correspondence, $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ has length at most $n-1$, so $r \leq n$. □

Corollary 18.2.1. *let R be an algebra of finite type over a field k. Then* $\dim(R) = \mathrm{trdeg}(\mathrm{Frac}(R)/k)$.

Proof. By the Noether normalization lemma, there is a finite extension $k[x_1, \ldots, x_n] \subseteq R$. Then $\dim(R) = n$. As localizations are flat, we have a finite extension of domains $k(x_1, \ldots, x_n) \subseteq R \otimes_{k[x_1,\ldots,x_n]} k(x_1, \ldots, x_n)$. Then $R \otimes_{k[x_1,\ldots,x_n]} k(x_1, \ldots, x_n)$ is in fact a field, so it equals $\mathrm{Frac}(R)$. Then $\mathrm{Frac}(R)/k(x_1, \ldots, x_n)$ is algebraic. □

19 More Dimension Theory

We begin with a key technical result for dimension counting.

Theorem 19.1 (Krull's Principal Ideal Theorem)**.** *Let R be a noetherian ring, $x \in R$. Then all minimal prime ideals containing (x) have codimension at most 1.*

Proof. Take a minimal prime ideal $\mathfrak{p} \supseteq (x)$. We want to show that $\dim(R_\mathfrak{p}) \leq 1$. Let $S = R_\mathfrak{p}$. Then S is a noetherian local ring containing x. By correspondence, the maximal ideal $\mathfrak{m} \subseteq S$ is a minimal prime ideal containing (x), so it is the only prime ideal containing (x). This tells us that $\mathrm{rad}((x)) = \mathfrak{m}$. Let $\mathfrak{q} \subsetneq \mathfrak{m}$ a prime ideal. If this doesn't exist, we have $\dim(S) = 0$ so we're done. Else, it suffices to show that $\mathfrak{q}$ has codimension 0. As $\mathrm{rad}((x)) = \mathfrak{m}$, we have $\mathrm{Spec}(R/(x)) = \mathrm{Spec}(R/\mathfrak{m}) =$ one point. Then $S/(x)$ is local of dimension 0. As it's noetherian, it is also artinian. We must now define the symbolic powers of an ideal.
We define the n^{th} symbolic power of $\mathfrak{q}$ to be the inverse image of $\mathfrak{q}^n S_\mathfrak{q}$ along the map $S \longrightarrow S_\mathfrak{q}$.

We denote this $\mathfrak{q}^{(n)}$. Clearly, $\mathfrak{q}^n \subseteq \mathfrak{q}^{(n)}$.
Returning to the problem, we have $\mathrm{rad}(x) = \mathfrak{m} \supsetneq \mathfrak{q}$. Then $x \notin \mathfrak{q}$, so x is a unit in the localization at $\mathfrak{q}$. Furthermore, we have the descending chain $(x) + \mathfrak{q}^{(1)} \supseteq (x) + \mathfrak{q}^{(2)} \supseteq \dots$. By artinianitudenessity of $S/(x)$, this must terminate. Thus, there exists an n such that $(x) + \mathfrak{q}^{(n)} = (x) + \mathfrak{q}^{(n+1)}$. Then any $f \in \mathfrak{q}^{(n)}$ equals some $ax + g$ for $a \in S$ and $g \in \mathfrak{q}^{(n+1)}$. Then $ax = f - g \in \mathfrak{q}^{(n)}$. As x is a unit in the localization, $a \in \mathfrak{q}^{(n)}$. Then as $x \in \mathfrak{m}$, we have $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + \mathfrak{m}\mathfrak{q}^{(n)}$. This tells us that $\mathfrak{q}^{(n)}/(\mathfrak{q}^{(n+1)} + \mathfrak{m}\mathfrak{q}^{(n)}) = 0$, so $(\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}) \otimes_S S/\mathfrak{m} = 0$. By Nakayama's lemma, this tells us that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Any ideal in $S_\mathfrak{q}$ is generated by its intersection with S, so this inequality implies that $\mathfrak{q}^n S_\mathfrak{q} = \mathfrak{q}^{n+1} S_\mathfrak{q}$. Then $\mathfrak{q}^n \otimes_{S_\mathfrak{q}} S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q} = 0$, so by Nakayama's lemma, $\mathfrak{q}^n S_\mathfrak{q} = 0$ This tells us that the unique maximal ideal of the local ring $S_\mathfrak{q}$ is nilpotent, so we may repeat the proof of artinian = noetherian plus dimension 0 and the fact that $S_\mathfrak{q}$ is noetherian to conclude that $S_\mathfrak{q}$ is noetherian, hence 0 dimensional. □

Corollary 19.1.1. *Let R be noetherian with $x_1, \dots, x_n \in R$. Then any minimal prime ideal containing $(x_1, \dots, x_n)$ has codimension at most n.*

Proof. Indeed, let $\mathfrak{p} \supseteq (x_1, \dots, x_n)$ be a minimal prime ideal. Let $\mathfrak{q} \subsetneq \mathfrak{p}$ be prime and maximal with respect to this property. Then some $x_i \notin \mathfrak{q}$. Without loss of generality, $x_1 \notin \mathfrak{q}$. Computing the codimension of $\mathfrak{p}$ comes down to computing the dimension of $R_\mathfrak{p}$, which is local with maximal ideal $\mathfrak{m} = \mathfrak{p}R_\mathfrak{p}$. Then $\mathfrak{p} = \mathrm{rad}(x_1, \dots, x_n)$. Furthermore, we have that $\mathrm{rad}(\mathfrak{q} + (x_1)) = \mathfrak{p}$. Then some $x_i^{r_i} = q_i + r_i x_1$, $q_i \in \mathfrak{q}$, $r_i \in R$. In $R/(y_2, \dots, y_n)$, Now take a minimal prime over the image of (x_1). Its pullback to R then contains $x_1, x_i^{r_i}$ for $i \geq 2$. Then, by minimality, it must be $\mathfrak{p}$, so $\mathfrak{p}$ is a minimal prime over (x_1) in $R/(y_2, \dots, y_n)$. Then its codimension here is at most 1 by Krull's principal ideal theorem, so the codimension of $\mathfrak{q}$ in the image is 0. Hence, it is a minimal prime over $(y_2, \dots, y_n)$, so by induction its codimension is at most $n - 1$. Then the codimension of $\mathfrak{p}$ is at most $n - 1$. □

Corollary 19.1.2. *Every noetherian local ring has finite dimension.*

Proof. Let $\mathfrak{m}$ be its maximal ideal. As R is noetherian, $\mathfrak{m} = (x_1, \dots, x_n)$. By the above corollary, $\mathrm{codim}(\mathfrak{m}) \leq n$, so $\dim(R) \leq n$. □

Remark. This fact was used implicitly in the above proof, but it's helpful to state explicitly that $\dim(R)$ is the supremum of the codimensions of maximal ideals.

We have then that noetherian rings are locally finite dimensional, but this turns out to not be a local property, even for noetherian rings. Indeed, there are noetherian rings that are not finite dimensional. For example, take $R = k[x_1, x_2, \dots]$. Let $\mathfrak{p}_1 = (x_1),]\mathfrak{p}_2 = (x_2, x_3), \mathfrak{p}_3 = (x_4.x_5, x_6, x_7), \dots$. Let $S = \bigcup_{n \geq 1} \mathfrak{p}_n$. Then take $R[S^{-1}]$.

Definition 19.1. A ring R is called catenary if for any $\mathfrak{p} \subseteq \mathfrak{q}$ prime ideals there exists a maximal chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{q}$ with r unique.

Theorem 19.2. *Let R be a catenary domain of finite dimension. Then for any prime ideal $\mathfrak{p}$, $\dim(R) = \mathrm{codim}(\mathfrak{p}) + \dim(R/\mathfrak{p})$.*

Proof. We have $0 \subseteq \mathfrak{p} \subseteq R$. As R is catenary, a maximal chain in R includes $\mathfrak{p}$, so we are done by correspondence. □

This definition becomes more grounded when considering the fact that finite type algebras over a field are catenary. We don't include the proof. We proceed now with a geometric characterization of a UFD.

Theorem 19.3. *Let R be a noetherian domain. Then R is a UFD if and only if all codimension 1 prime ideals are principal. To give some more exposition, a codimension 1 prime ideal in a domain is a minimal nonzero prime ideal. This corresponds to a maximal proper irreducible closed subset of* $\operatorname{Spec} R$. *Note that* $\operatorname{Spec} R$ *is irreducible in a domain. This condition then says that the geometric interpretation of a noetherian UFD is that any maximal proper irreducible closed subset of* $\operatorname{Spec} R$ *is defined by one equation.*

Proof. Let R be a noetherian UFD. Let $\mathfrak{p}$ be a codimension 1 prime ideal. This says that $0 \subsetneq \mathfrak{p}$ is a maximal chain. Let $x \neq 0$ in $\mathfrak{p}$. As R is a UFD, $x = f_1 \dots f_r$ irreducibles. By primality, some $_i \in \mathfrak{p}$. Then we have $0 \subsetneq (f_i) \subseteq \mathfrak{p}$. As R is a UFD, (f_i) is prime, so $(f_i) = \mathfrak{p}$ as desired. Note that this did not use the noetherian condition.
Conversely, suppose all codimension 1 prime ideals are principal. First, let $f \in R$ be a nonzero nonunit. Suppose that f has no irreducible decomposition. In particular, f is reducible, so $f = f_1 g_1$ for f_1, g_1 nonzero nonunits. Then at least one of these has no irreducible factorization. Without loss of generality, f_1 has no irreducible factorization. Then f_1 is a nonzero nonunit with no irreducible factorization. These are the same assumptions we had on f, so we repeat this process to yield $f_1 = f_2 g_2$ nonzero nonunits with f_2 having no irreducible factorization. This yields the chain $(f) \subseteq (f_1) \subseteq (f_2) \subseteq \dots$. These inclusions are strict as the g_i are also assumed to be nonunits. This contradicts noetherianitude, so all nonzero nonunits have an irreducible factorization. Note that this argument holds in any noetherian ring.
We now put the U in UFD. We first claim that for $f \in R$ irreducible that (f) is prime. Indeed, f is not a unit so $(f) \subsetneq R$. One can show that any nonempty set of prime ideals in a noetherian ring contains a minimal element. We show that any decreasing chain of primes stabilizes, which certainly implies the minimality condition. Indeed, let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots$ be a chain of primes. By noetherinitude, $\mathfrak{p}_1 = (x_1, \dots, x_n)$. Then by Krull's principal ideal theorem (or rather its corollary), $\operatorname{codim}(\mathfrak{p}_1) \leq n$. In particular, any chain of primes ending in $\mathfrak{p}_1$ stabilizes, so this chain does. Now, we can let $\mathfrak{p} \supseteq (f)$ be a minimal prime. By Krull's principal ideal theorem, it has codimension at most one. As $0 \subsetneq (f) \subseteq \mathfrak{p}$, the codimension of $\mathfrak{p}$ is 1. Thus, by assumption, it's principal so $\mathfrak{p} = (g)$. Then $f = gh$ for some $h \in R$. As f is irreducible and g is not a unit, h is a unit so $(f) = (g)$ is prime. Now let $f_1 \dots f_r = g_1 \dots g_s$ irreducibles. Then $g_1 \dots g_s \in (f_1)$, which is prime as above. Then some $g_i \in (f_1)$. As these are irreducible, $g_i \approx f_1$. The result follows by induction. □

Remark. For a noetherian normal domain R, one can define an abelian group called the divisor class group $\mathrm{CL}(R)$ which is generated by all codimension 1 prime ideals such that $\mathrm{CL}(R) = 0$ if and only if all codimension 1 primes are principal if and only if R is a UFD. This measures the obstruction to being a UFD.

20 Regular Local Rings

To try and define a regular local ring, we must first prove the following lemma.

Lemma 20.1. *Let $(R, \mathfrak{m})$ be a noetherian local ring. Let k $R/\mathfrak{m}$ its residue field. Then* $\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Proof. As R is noetherian, $\mathfrak{m}$ is finitely generated, so $\dim_k(\mathfrak{m}/\mathfrak{m}^2) < \infty$. Indeed, let $e_1, \ldots, e_n$ be a k-basis for $\mathfrak{m}/\mathfrak{m}^2$. We lift these to $\mathfrak{m}$ but call them the same thing. By Nakayama's lemma, $\mathfrak{m} = (e_1), \ldots, e_n)$. By Krull's principal ideal theorem, $\operatorname{codim}(\mathfrak{m}) \leq n$. Thus, $\dim(R) \leq n = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. □

Definition 20.1. A noetherian local ring R is called regular if $\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ for k the residue field of R.

Example. A regular local ring R of dimension 0 has $\mathfrak{m} = \mathfrak{m}^2$, so by Nakayama's lemma, $\mathfrak{m} = 0$. Then R is a field. For example, $k[x]/(x^n)$ has dimension 0 but is not regular for $n \geq 2$.

It is a fact that regular local rings are domains. Given this, regular local rings of dimension 1 are precisely discrete valuation rings.

Example. $R = k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$ is a regular local ring. Indeed, its maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. Then $\mathfrak{m}^2 = (x_1^2, x_1x_2, \ldots, x_n^2)$ the ideal of homogeneous polynomials of total degree at least 2. Then $\mathfrak{m}/\mathfrak{m}^2$ has k dimension n, and k is the residue field of R. Furthermore, we have the chain $0 \subsetneq (x_1) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n)$, so $\dim(R) \geq n$. Furthermore, as $\dim(k[x_1, \ldots, x_n]) = n$, by correspondence we have $\dim(R) \geq n$. Then $\dim(R) = n = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Lemma 20.2. *Let R be a ring, with $a \geq 0$ and $\mathfrak{m}$ a maximal ideal. Then* $R/\mathfrak{m}^a \cong R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^a$.

Proof. Note that $R/\mathfrak{m}^a$ is local with maximal ideal $\mathfrak{m}$. Then localizing this at $\mathfrak{m}$ does nothing. Consider the exact sequence

$$0 \longrightarrow \mathfrak{m}^a \longrightarrow R \longrightarrow R/\mathfrak{m}^a \longrightarrow 0$$

Localizing this at $\mathfrak{m}$ yields

$$0 \longrightarrow \mathfrak{m}^a \otimes_R R_{\mathfrak{m}} \longrightarrow R_{\mathfrak{m}} \longrightarrow (R/\mathfrak{m}^a)_{\mathfrak{m}} \longrightarrow 0$$

which becomes

$$0 \longrightarrow \mathfrak{m}^a R_{\mathfrak{m}} \longrightarrow R_{\mathfrak{m}} \longrightarrow R/\mathfrak{m}^a \longrightarrow 0$$

as discussed above. Then by exactness we have $R/\mathfrak{m}^a \cong R_{\mathfrak{m}}/\mathfrak{m}^a R_{\mathfrak{m}}$ as desired. □

We now proceed with a discussion of the subvarieties of $\mathbb{A}^2_{\mathbb{C}}$. Let Y be such a subvariety. If its dimension is 2, then it is of course the whole affine plane. If it is dimension 0, it is a maximal ideal, hence a point by the Nullstellensatz. Now, if Y has dimension 1, its corresponding prime ideal has codimension 1, and is therefore principal. as $\mathbb{C}[x, y]$ is a UFD. Thus, Y is defined by a single equation defined by an irreducible polynomial. This is not so easy in higher dimensions. Indeed, in $\mathbb{A}^3_{\mathbb{C}}$, there are dimension 1 varieties which cannot be defined by a single equation.

Lemma 20.3 (Prime avoidance lemma)**.** *Let $n \geq 1$, $I_1, \ldots, I_n, J \subseteq R$ ideals with all but (at most) 1 of the I_j are prime. If $J \subseteq \bigcup I_j$, then $J \subseteq I_a$ some a.*

Proof. We proceed by induction. The case $n = 1$ is immediate. Suppose without loss of generality that I_n is prime. We may assume that J is not contained in any union of $n-1$ of the I_j, as otherwise by induction we are done. Then let $x_a \in J - \bigcup_{b \neq a} I_b$. Certainly, $x_a \in I_a$. Consider $y = x_1 \ldots x_{n-1} + x_n \in J$. Then $y \in I_a$ for some a. If $1 \leq a \leq n-1$, then $x_1 \ldots x_{n-1} \in I_a$ However, $x_n \notin I_a$, a contradiction. Thus, we assume $a = n$. By primality, $x_1 \ldots x_{n-1} \notin I_n$, yet $y, x_n \in I_n$ a contradiction. □

Lemma 20.4. *Let $(R, \mathfrak{m})$ be a noetherian local ring. Then $\dim(R)$ is the smallest r such that there exist $f_1, \ldots, f_r \in \mathfrak{m}$ such that $\mathfrak{m} = \operatorname{rad}(f_1, \ldots, f_r)$.*

Proof. By Krull's principal ideal theorem, if $\operatorname{rad}(f_1, \ldots, f_r) = \mathfrak{m}$ then $\dim(R) = \operatorname{codim}(\mathfrak{m}) \leq r$ as R is local. On the other hand, it suffices to find $r = \dim(R)$ many elements of $\mathfrak{m}$ such that $\operatorname{rad}(f_1, \ldots, f_r) = \mathfrak{m}$. By induction, it suffices to show that there exists an $f \in \mathfrak{m}$ with $\dim(R/(f)) < \dim(R)$. We claim that any f not in any minimal prime ideal satisfies this. Indeed, let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a maximal chain. Then $\mathfrak{p}_0$ is a minimal prime ideal. A chain in $R/(f)$ corresponds to a chain in R whose bottom element contains f. Thus, such a chain cannot be maximal as f is not in any minimal prime. Thus, it suffices to find such an f. As $\dim(R) > 0$, $\mathfrak{m}$ is not a minimal prime ideal. By prime avoidance, as $\mathfrak{m}$ is not contained in any minimal prime, $\mathfrak{m}$ is not contained in any finite union of minimal primes, so such an f exists as R has only finitely many minimal primes. □

Examples. 1. Field = RLR + dimension 0

2. Discrete valuation rings are RLRs

3. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/(p^n)$

Definition 20.2. A system of parameters in a noetherian local ring $(R, \mathfrak{m})$ is a sequence of elements $f_1, \ldots, f_r \in \mathfrak{m}$ with $r = \dim(R)$ and $\operatorname{rad}(f_1, \ldots, f_r) = \mathfrak{m}$. We have proven before that these exist.

Lemma 20.5. *Let $(R, \mathfrak{m})$ be a noetherian local ring. For any $f \in \mathfrak{m}$, $\dim(R/(f)) \geq \dim(R) - 1$. For f not a zero divisor, equality is attained.*

Proof. Let $r = \dim(R)$, $s = \dim(R/(f))$. Take a system of parameters $g_1, \ldots, g_s \in R/(f)$. Then $\mathfrak{m}$ is nilpotent in $R/(f, g_1, \ldots, g_s)$, so $\operatorname{rad}(f, g_1, \ldots, g_s) = \mathfrak{m}$, so $s + 1 \geq \dim(R)$. Now, suppose f is not a zero divisor. Then we have the desired equality if f is not contained in any

minimal prime ideal of R. Indeed, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the minimal primes of R. Suppose $f \in \mathfrak{p}_1$. Then for $j \geq 2$ there exists $x_j \in \mathfrak{p}_j - \mathfrak{p}_1$. Then by primality, $g = x_2 \ldots x_n \in \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_n - \mathfrak{p}_1$. Then $fg \neq 0$ as f is not a zero divisor, so it must be in $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = \mathrm{nil}(R)$. Then there is some m with $f^m g^m = 0$, but as f is not a zero divisor we have $g^m = 0$ so $g \in \mathrm{nil}(R)$, but $g \notin \mathfrak{p}_1$, a contradiction. □

Theorem 20.6. *A regular local ring is a domain.*

Proof. Noetherian local rings are finite dimensional, so we proceed by induction on the dimension. Indeed,as discussed above, 0 dimensional regular local rings are fields, hence domains. Suppose now that $\dim(R) = r > 0$. Then $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = r > 0$, so $\mathfrak{m} \nsubseteq \mathfrak{m}^2$. R has finitely many minimal prime ideals, so by prime avoidance, $\mathfrak{m}$ is not contained in $\mathfrak{m}^2$ union the minimal prime ideals, as if so it wuld be contained in some monimal prime, hence equal some minimal prime. That would imply, as R is local, that this is the only prime ideal. Hence, all primes would be maximal so $\dim(R) = 0$, a contradiction. Thus, we have some $f \in \mathfrak{m}$ not in $\mathfrak{m}^2$ union the minimal primes. By the proof of the previous lemma, $\dim(R/(f)) = r - 1$.
We seek to show that $S = R/(f)$ is a regular local ring. It's certainly noetherian and local, with maximal ideal $\mathfrak{m}_S = \mathfrak{m}S$. Then the residue field of S is $(R/(f))/(\mathfrak{m}/(f)) = k$. It therefore suffices to show that $\dim_k(\mathfrak{m}_S/\mathfrak{m}_S^2)$. Indeed, this is true as $\mathfrak{m}_S/\mathfrak{m}_S^2 = (\mathfrak{m}/\mathfrak{m}^2)/(f)$ and f is nonzero in $\mathfrak{m}/\mathfrak{m}^2$. Then S is a regular local ring, so by induction it's a domain. Then (f) is a prime ideal. Then there exists some $\mathfrak{p} \subseteq (f)$ a minimal prime ideal. Then any $y \in \mathfrak{p}$ equals some zf, $z \in R$. By primality, z or f must be in $\mathfrak{p}$. However, by definition, f is not contained in any minimal prime ideal, so in particular $f \notin \mathfrak{p}$. Then $z \in \mathfrak{p}$ so $\mathfrak{p} = \mathfrak{p}f$. Furthermore, as f is not contained in any minimal prime, it is not properly contained in any prime. Thus, it must equal $\mathfrak{m}$, so $\mathfrak{p} = \mathfrak{p}\mathfrak{m}$, so by Nakayama's lemma $\mathfrak{p} = 0$ so R is a domain. □

Definition 20.3. A regular sequence in R is a sequence $f_1, \ldots, f_n \in R$ 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 $R/(f_1, f_2)$, etc.

Theorem 20.7. *Let $(R, \mathfrak{m})$ be a noetherian local ring. Then R is regular if and only if $\mathfrak{m}$ is generated by a regular sequence.*

Remark. Using some homological algebra, this leads to the characterization that R is regular if and only if it has finite global dimension, i.e. every module over R has a finite projective resolution. This leads to (Auslander-Buchsbaum, Serre, 1956), which states that the localization of a regular ring at a prime ideal is regular. This also yields that regular local rings are UFDs.

Proof. Let $(R, \mathfrak{m})$ be a regular local ring of dimension n. Let $f_1, \ldots, f_n \in \mathfrak{m}$ map to a k basis of $\mathfrak{m}/\mathfrak{m}^2$. By Nakayama's lemma, they generate $\mathfrak{m}$. We claim that this is a regular sequence. Indeed, as proven before R is a domain so as no f_i is 0 due to linear independence in $\mathfrak{m}/\mathfrak{m}^2$, they are not zero divisors. By an earlier lemma, $S = R/(f_1)$ has dimension $n - 1$. Furthermore, $\mathfrak{m}_S/\mathfrak{m}_S^2 = (\mathfrak{m}/\mathfrak{m}^2)/kf_1$, which has k dimension $n - 1$, so S is a regular local ring. Then S is a domain. By linear independence, f_2 is nonzero in S, hence not a zero divisor.

Conversely, suppose that $\mathfrak{m}$ is generated by a regular sequence $f_1, \ldots, f_n$. We have that $\dim(R/(f_1)) = \dim(R) - 1$. Also, $\dim(R/(f_1, f_2)) = \dim\left(\frac{R/(f_1)}{(f_2)}\right) = \dim(R/(f_1)) - 1 = \dim(R) - 2$. Hence, $0 = \dim(R/\mathfrak{m}) = \dim(R/(f_1, \ldots, f_n)) = \dim(R) - n$, so we have $\dim(R) = n$. We then want to show that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = n$. By Nakayama's lemma it suffices to show that $(f_1, \ldots, f_n)$ is a minimal set of generators for $\mathfrak{m}$. Indeed, if $(g_1, \ldots g_{n-1}) = \mathfrak{m}$ then by Krull's principal ideal theorem, we have $\operatorname{codim}(\mathfrak{m}) \leq n - 1$, but $\operatorname{codim}(\mathfrak{m}) = \dim(R) = n$, a contradiction. $\square$