$\int$(͡° ͜ʖ ͡°)dx

MA 526

Commutative Algebra

Notes By: Aryaman Maithani

Spring 2020-21

Last Updated: March 22, 2021

Contents

Notation

1. $\mathcal{N}(R)$ denotes the nilradical of R.
2. $\mathcal{J}(R)$ denotes the Jacobson radical of R.
3. $\operatorname{Spec}(R)$ denotes the set of prime ideals of R.
4. $\operatorname{mSpec}(R)$ denotes the set of maximal ideals of R.
5. $N \leq M$ is read as "N is a submodule of M."
6. $I \trianglelefteq R$ is read as "I is an ideal of R."
7. For an integral domain R, $Q(R)$ denotes its field of fractions.
8. k denotes a field. If k is algebraically closed, we write this as $\mathsf{k} = \overline{\mathsf{k}}$.

Lecture 1. Associated primes of ideals and modules

Definition 1.1. Suppose M, N are R-submodules of some R-module M'. Then,

$$M :_R N := \{r \in R \mid rN \subset M\}.$$

Definition 1.2. Let M be an R-module and $0 \neq x \in M$. If $\mathfrak{p} = 0 :_R x$ is a prime in R, then we say that $\mathfrak{p}$ is an associated prime of M.

$$\mathrm{Ass}_R(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} = 0 :_R x \text{ for some } x \in M \setminus \{0\}\}.$$

Definition 1.3. The elements of $\mathrm{Ass}(M)$ which are not minimal in $\mathrm{Ass}(M)$ are called embedded primes.

Definition 1.4. Fix $x \in X$. The map $\mu_x : R \to M$ defined by $r \mapsto rx$ is called the homothety by x.

Note that $\ker \mu_x = 0 :_R x$.

Proposition 1.5. A prime $\mathfrak{p}$ is an associated prime of M iff $R/\mathfrak{p}$ is isomorphic to a submodule of M.

Definition 1.6. $a \in R$ is a zero divisor on M if $ax = 0$ for some $0 \neq x \in M$.

$$\mathcal{Z}(M) := \{a \in R \mid a \text{ is a zero divisor on } M\}.$$

If a is not a zero divisor, then μ_a is called a non zero divisor on M or M-regular.

Note that a is a zero divisor iff μ_a is not injective.

Proposition 1.7. Let R be Noetherian and $M \neq 0$ finitely generated R-module. Then,

1. the maximal elements among $\{(0 : x) \mid x \neq 0\}$ are prime. In particular, $\mathrm{Ass}\, M \neq \emptyset$.
2. $\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$.

Example 1.8. Let $R = \Bbbk[x,y]$ for a field $\Bbbk$ and put $I = \langle x^2, xy\rangle$. Then, $\operatorname{Ass}(R/I) = \{\langle x\rangle, \langle x,y\rangle\}$. Note that $\langle x\rangle$ is not maximal among the annihilators.

Proposition 1.9. Let $S \subset R$ be a multiplicatively closed set. Then,

1. $\operatorname{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}(M),\ \mathfrak{p} \cap S = \varnothing\}$.
2. $\mathfrak{p} \in \operatorname{Ass}_R(M) \iff \mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$.

Definition 1.10. $\operatorname{Supp}(M) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}$.

Proposition 1.11. If M is finitely generated, then $\operatorname{Supp}(M) = V(\operatorname{ann} M)$.

Proposition 1.12. If $0 \to N \to M \to L \to 0$ is exact, then $\operatorname{Supp} M = \operatorname{Supp} N \cup \operatorname{Supp} L$.

Proposition 1.13. Let L, K be f.g. R-modules. Then, $\operatorname{Supp}(K \otimes_R L) = \operatorname{Supp} L \cap \operatorname{Supp} K$. In particular, $\operatorname{Supp}(M/IM) = \operatorname{Supp} M \cap V(I)$.

Proposition 1.14. $\operatorname{Ass}(M) \subset \operatorname{Supp}(M)$.

Note that if R is Noetherian and $I \trianglelefteq R$ is an ideal, then $\operatorname{Ass}(R/I) \subset \operatorname{Supp}(R/I) = V(I)$.

Assume that R and M are Noetherian from now.

Proposition 1.15. $\operatorname{Ass} M$ and $\operatorname{Supp} M$ have the same set of minimal primes.

Remark 1.16. Note that $\mathfrak{p}$ is a minimal prime over $\mathfrak{p}^n$. That is, it is a minimal element of $V(\mathfrak{p}^n) = \operatorname{Supp}(R/\mathfrak{p}^n)$ and hence, an element of $\operatorname{Ass}(M/\mathfrak{p}^n)$.

Note that $V(\mathfrak{p}^n) = \operatorname{Supp}(R/\mathfrak{p}^n)$ is true because of the Noetherian assumption.

Theorem 1.17.

1. There exists a sequence of R-submodules of M
$$(0) = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

such that $M_{i+1}/M_i \cong R/\mathfrak{p}_i$ for $\mathfrak{p}_i \in \operatorname{Spec}(R)$.

2. Given any sequence as above, we have

$$\operatorname{Ass} M \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \operatorname{Supp} M.$$

In particular, $\operatorname{Ass} M$ is always finite and hence, the set of minimal primes over any ideal is finite.

Definition 1.18. Let $N \leq M$ be a submodule such that $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$. Then, M is called $\mathfrak{p}$-primary.

Definition 1.19. Let M be a module such that $\operatorname{Ass} M = \{\mathfrak{p}\}$. Then, M is called $\mathfrak{p}$-coprimary.

Example 1.20. If $\mathfrak{m} \subset R$ is maximal, then $\mathfrak{m}^n$ is $\mathfrak{m}$-primary for all $n \geq 1$.
If $\mathfrak{p} \subset R$ is prime, then $\mathfrak{p}^n$ need not be $\mathfrak{p}$-primary.

Proposition 1.21. If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal of R, then $\mathfrak{q}R_{\mathfrak{p}}$ is a $\mathfrak{p}R_{\mathfrak{p}}$-primary ideal.

Proof. Note that $(R/\mathfrak{q})_{\mathfrak{p}} \cong R_{\mathfrak{p}}/\mathfrak{q}R_{\mathfrak{p}}$ as $\mathbb{R}_{\mathfrak{p}}$-modules. By Proposition 1.9, we see that

$$\begin{aligned} \mathfrak{a}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/\mathfrak{q}R_{\mathfrak{p}}) &\iff \mathfrak{a}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}}\left((R/\mathfrak{q})_{\mathfrak{p}}\right) \\ &\iff \mathfrak{a} \in \operatorname{Ass}_R(R/\mathfrak{q}) = \{\mathfrak{p}\} \\ &\iff \mathfrak{a} = \mathfrak{p} \end{aligned}$$

and hence, $\mathfrak{q}R_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$-primary. □

Definition 1.22. For $a \in R$, define $\mu_a : M \to M$ as $x \mapsto ax$.

Definition 1.23.

$$\begin{aligned} \operatorname{nil}(M) &:= \{a \in R \mid \mu_a \text{ is nilpotent}\} \\ &= \{a \in R \mid a^n M = 0 \text{ for some } n\} \\ &= \sqrt{\operatorname{ann} M} \end{aligned}$$

Proposition 1.24. If $\operatorname{Ass}(M) = \{\mathfrak{p}\}$, then $\mathcal{Z}(M) = \operatorname{nil} M = \sqrt{\operatorname{ann} M}$.

Theorem 1.25. $|\operatorname{Ass} M| = 1 \iff \mathcal{Z}(M) = \operatorname{nil} M$.
If either condition holds, we have $\operatorname{Ass} M = \{\sqrt{\operatorname{ann} M}\}$.

Corollary 1.26. If $N \leq M$ is $\mathfrak{p}$-primary, then $\operatorname{Ass}(M/N) = \{\sqrt{\operatorname{ann} M/N}\}$.

Corollary 1.27. I is $\mathfrak{p}$-primary implies $\mathfrak{p} = \sqrt{I}$.

Remark 1.28. Note that if $\sqrt{I}$ is prime, it does not imply that I is $\sqrt{I}$-primary.

Corollary 1.29. I is $\mathfrak{p}$-primary iff $\bigcup_{\mathfrak{p} \in \operatorname{Ass}(R/I)} \mathfrak{p} = \mathcal{Z}(R/I) = \operatorname{nil}(R/I) = I$.

Proposition 1.30. If N_1 and N_2 are $\mathfrak{p}$-primary, so is $N_1 \cap N_2$.

Definition 1.31. A submodule $N \leq M$ is called reducible if $N = N_1 \cap N_2$ with $N_1 \neq N \neq N_2$. It is called irreducible otherwise.

Proposition 1.32. Prime ideals are irreducible.

Theorem 1.33. Proper irreducible submodules are primary.

Theorem 1.34. Any proper submodule can be written as an intersection of finitely many irreducible submodules.

Corollary 1.35. Let R be a Noetherian ring and M a Noetherian R-module. If $N \lneq M$ is a proper R-submodule, then N can be written as

$$N = N_1 \cap \cdots \cap N_r,$$

where $N_1, \ldots, N_r$ are primary submodules.

The above is called a primary decomposition of N.

Definition 1.36. A primary decomposition is called minimal if $\mathrm{Ass}(M/N_i) \neq \mathrm{Ass}(M/N_j)$ for $i \neq j$.

It is called irredundant if N_i can be removed.

Theorem 1.37. If $N = N_1 \cap \cdots \cap N_r$ is an irredundant primary decomposition and $\mathrm{Ass}(M/N_i) = \{\mathfrak{p}_i\}$, then $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Theorem 1.38. If $\mathfrak{p}$ is a minimal associated prime of M/N, then the $\mathfrak{p}$-primary component of N is $\varphi_{\mathfrak{p}}^{-1}(N\mathfrak{p})$, where $\varphi_{\mathfrak{p}} : M \to M_{\mathfrak{p}}$ is the natural map $x \mapsto \frac{x}{1}$.

In particular, the component corresponding to the minimal prime is uniquely determined.

Lecture 2. Artinian rings and Artinian modules

We now drop the assumption from the previous chapter of rings and modules being Noetherian.

Definition 2.1. An R-module M is called Artinian if every descending chain of R-submodules of M stabilises.

R is said to be an Artinian ring if R is Artinian as an R-module.

Proposition 2.2. Let $\Bbbk$ be a field and V a $\Bbbk$-module, i.e., a $\Bbbk$-vector space. Then, V is Artinian iff V is finite dimensional iff V is Noetherian.

Proposition 2.3. Let R be an Artinian ring.

1. If I is an ideal of R, then R/I is an Artinian ring.
2. If R is an integral domain, then R is a field.
3. More generally, every non zero divisor of R is a unit.
4. If $\mathfrak{p} \in \operatorname{Spec}(R)$, then $\mathfrak{p}$ is maximal. That is, $\operatorname{Spec}(R) = \operatorname{mSpec}(R)$.
   Thus, $\mathcal{N}(R) = \mathcal{J}(R)$.
5. R has finitely many maximal ideals. (It may have infinitely many ideals, however.)
6. If $I \trianglelefteq R$, then $\operatorname{Ass}(R/I) = \operatorname{Supp}(R/I) = V(I)$.
7. If $N = \mathcal{N}(R)$, then there exists k such that $N^k = 0$.
8. Let $0 \to N \to M \to L \to 0$ be an exact sequence. Then M is Artinian iff N and L are Artinian.
   In particular, $\bigoplus_{i=1}^n M_i$ is Artinian iff each M_i is.
9. If M is a finitely generated R-module, then M is an Artinian R-module and $R/\operatorname{ann} M$ is an Artinian ring.

Proposition 2.4. Let M be an R-module and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \in \operatorname{mSpec} R$ are maximal ideals such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$. Then,
M is Noetherian $\iff$ M is Artinian.

Note that the maximal ideals above need not be distinct. Moreover, R is not assumed to be Artinian.

Proposition 2.5. Let R be an Artinian ring. Then, R is Noetherian ring.

Proposition 2.6. Let R be a Noetherian ring with $\operatorname{Spec} R = \operatorname{mSpec} R$. Then, R is an Artinian ring.

Proposition 2.7. If R is Artinian and M an Artinian R-module, then M is a Noetherian R-module. In particular, M is finitely generated.

Theorem 2.8. Let R be an Artinian ring. Then, there exist uniquely determined Artinian local rings $R_1, \ldots, R_n$ such that

$$R \cong R_1 \times \cdots \times R_n.$$

Definition 2.9. An R-module $M \neq 0$ is called simple if the only R-submodules of M are 0 and M.

Proposition 2.10. An R-module M is simple iff $M \cong R/\mathfrak{m}$ for some $\mathfrak{m} \in \operatorname{mSpec} R$. The isomorphism is as R-modules. In particular, M is cyclic.

Lemma 2.11. A simple module is both Noetherian and Artinian.

Definition 2.12. Let M be an R-module. A series of the form

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$$

is called a composition series if M_{i+1}/M_i is simple for each i. n is called the length of this composition series.

Note that a composition series has finite length, by definition.

Theorem 2.13. M has a composition series $\iff$ M is Artinian and Noetherian.

Definition 2.14. Let $M \neq 0$ be an R-module. Define

$$l_R(M) := \min\{n \mid M \text{ has a composition series of length } n\}.$$

$l_R(M) = \infty$ if the set on the right is empty. $l_R(M)$ is called the length of M over R.

Note that if $R = \mathsf{k}$ is a field, then the length of M is simply the dimension.

Definition 2.15. If $l_R(M) < \infty$, then M is called a finite length module.

Proposition 2.16. M is a finite length module iff M is Artinian and Noetherian.

Proposition 2.17. Let R be a Noetherian ring and M a finite length R-module. Then, $\operatorname{Ass}(M) \subset \operatorname{mSpec}(R)$.

Proposition 2.18. Let M be a finite length module and $N \leq M$. Then, N also has finite length and $l_R(N) \leq l_R(M)$ with equality iff $N = M$.

Theorem 2.19 (Jordan-Hölder)**.** Every composition series of a finite length module M has the same length.

Now, if

$$\begin{aligned} 0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M, \\ 0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_{n-1} \subsetneq N_n = M \end{aligned}$$

are two composition series of M, then there exists a permutation $\sigma \in S_n$ such that

$$M_i / M_{i-1} \cong N_{\pi(i)} / N_{\pi(i)-1}$$

for all $1 \leq i \leq n$. In other words, the quotients that appear are the same.

Proposition 2.20. Let M be a finite length module. Any series of the form

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$$

is actually a composition series.

Proposition 2.21. Let $0 \to N \to M \to L \to 0$ be an exact sequence. Then, $l_R(M) = l_R(N) + l_R(L)$.

Note that M is finite length iff N and L both are.

Proposition 2.22. If R is Noetherian and M a finite length R-module, then $\mathrm{Ass}(M) \subset \mathrm{mSpec}(R)$.

Lecture 3. Integral Extensions of Rings

Definition 3.1. Let $R \subset S$ be non-zero commutative rings. An element $s \in S$ is called integral over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$.

Let
$$T = \{s \in S \mid s \text{ is integral over } R\}.$$
T is called the integral closure of R in S.

If R is an integral domain and $S = Q(R)$, then T is called the normalisation of R. R is called normal or integrally closed if $T = R$.

Recall that if R is an integral domain, then $Q(R)$ denotes the field of fractions of R.

We shall shortly show that T is a subring of S.

Theorem 3.2. If R is a UFD, then R is integrally closed. In other words, UFDs are normal.

The converse is not true.

Theorem 3.3 (Cayley-Hamilton)**.** Let $I \trianglelefteq R$ be an ideal and M a finitely generated R-module. Let $\varphi : M \to M$ be an R-endomorphism such that $\varphi(M) \subset IM$. Then, φ satisfies a monic polynomial of the form
$$x^n + a_1 x^{n-1} + \cdots + a_n$$
with $a_1, \ldots, a_n \in I$.

Corollary 3.4 (Nakayama)**.** Suppose M is finitely generated over R and $I \trianglelefteq R$ is such that $M = IM$. Then, there exists $a \in I$ such that $(1 + a)M = 0$.
In particular, if $I \subset \mathcal{J}(R)$, then $M = 0$.

Corollary 3.5. If $\varphi : M \to M$ is a surjective R-linear map, then φ is an isomorphism. (M is finitely generated as usual.)

Corollary 3.6. Suppose $M \cong R^n$. Then, any set of n generators is linearly independent.

Corollary 3.7. Let R be a non-zero commutative ring. Then, $R^n \cong R^m$ (as R-modules) iff

$n = m$.

Theorem 3.8. Let $R \subset S$ be non-zero commutative rings and $s \in S$. TFAE:

1. s is integral over R.
2. $R[s]$ is a finitely generated as an R-module.
3. There exists a subring T such that $R[s] \subset T \subset S$ and T is a finitely generated R-module.

Theorem 3.9. Let $R \subset S$ be a ring extension and $T = \overline{R}^S$ the integral closure of R in S. Then, T is a subring of S.

Proposition 3.10. If $R \subset T$ and $T \subset S$ are integral extensions, then so is $R \subset S$.

Corollary 3.11. If T is the integral closure of R in S, then the integral closure of T in S is T.

Symbolically, if $T = \overline{R}^S$, then $\overline{T}^S = T$.

Note that if $R \subset S$ is a ring extension and $I \trianglelefteq S$ is an ideal, then $I^c = R \cap I$ is an ideal of R. (Called the contraction.) Also, one has the natural inclusion and projection maps as

$$R \overset{i}{\hookrightarrow} S \overset{\pi}{\twoheadrightarrow} S/I.$$

Then, $I^c = \ker(\pi \circ i)$ and hence, R/I^c is isomorphic to a subring of S/I. We denote this inclusion by writing $R/I^c \hookrightarrow S/I$.

Proposition 3.12. If $R \subset S$ is an integral extension, then so is $R/I^c \hookrightarrow S/I$.

Definition 3.13. Suppose $\varphi : R \to S$ is a ring map. Then, φ is called integral if $\varphi(R) \subset S$ is an integral extension.

Proposition 3.14. Let $U \subset R$ be a multiplicatively closed subset and let $R \subset S$ be an integral extension. Then, $U^{-1}R \subset U^{-1}S$ is an integral extension.

Proposition 3.15. Let R be an integral domain. TFAE:

1. R is integrally closed (normal).
2. $R_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \operatorname{Spec}(R)$.
3. $R_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \in \operatorname{mSpec}(R)$.

Lemma 3.16. Let $R \subset S$ be an integral extension of integral domains.
Then, R is a field $\iff$ S is a field.

Corollary 3.17. Let $R \subset S$ be rings (not necessarily domains) and $\mathfrak{q} \in \operatorname{Spec} S$. Define $\mathfrak{p} := R \cap \mathfrak{q}$.
Then, $\mathfrak{p} \in \operatorname{mSpec} R \iff \mathfrak{q} \in \operatorname{mSpec} S$.

In particular, given an integral extension, the contraction of a maximal ideal is maximal.

Definition 3.18. Let $R \subset S$ be rings. Suppose $Q \in \operatorname{Spec} S$ and $P \in \operatorname{Spec} R$. Q is said to lie over P if $Q^c = Q \cap R = P$.

Theorem 3.19 (Lying over theorem)**.** Let $R \subset S$ be an integral extension of rings and $\mathfrak{p} \in \operatorname{Spec} R$. Then, there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.

In other words: Given an integral extension, there is always a prime lying over a prime.

Theorem 3.20 (Going up theorem)**.** Let $R \subset S$ be an integral extension. Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} R$ with $\mathfrak{p}_1 \subset \mathfrak{p}_2$ and $\mathfrak{q}_1 \in \operatorname{Spec} S$ be such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Then, there exists $\mathfrak{q}_2 \in \operatorname{Spec} S$ such that $\mathfrak{q}_1 \subset \mathfrak{q}_2$ and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$.

$$\begin{array}{r} S \\ \text{int}\,\Big| \\ R \end{array} \qquad\qquad \begin{array}{ccc} \mathfrak{q}_1 & \subset & \exists\mathfrak{q}_2 \\ \Big| & & \vdots \\ \mathfrak{p}_1 & \subset & \mathfrak{p}_2 \end{array}$$

In fact, inductively, we see that any chain above can be "completed."

$$\begin{array}{r} S \\ \text{int}\,\Big| \\ R \end{array} \qquad \begin{array}{ccccccccccccc} \mathfrak{q}_1 & \subset & \mathfrak{q}_2 & \subset & \cdots & \subset & \mathfrak{q}_m & \subset & \exists\mathfrak{q}_{m+1} & \subset & \cdots & \subset & \exists\mathfrak{q}_n \\ \Big| & & \Big| & & & & \Big| & & \vdots & & & & \vdots \\ \mathfrak{p}_1 & \subset & \mathfrak{p}_2 & \subset & \cdots & \subset & \mathfrak{p}_m & \subset & \mathfrak{p}_{m+1} & \subset & \cdots & \subset & \mathfrak{p}_n \end{array}$$

Proposition 3.21 (Incompatibility (INC))**.** Let $R \subset S$ be an integral extension of rings. Let $Q_1, Q_2 \in \operatorname{Spec} S$ lie over $P \in \operatorname{Spec} R$. If Q_1 and Q_2 are distinct, then they are incomparable. That is, $Q_1 \neq Q_2 \implies Q_1 \not\subset Q_2$ and $Q_2 \not\subset Q_1$.

$$
\begin{tikzcd}
S \arrow[d, dash, "\text{int}"'] & Q_1 \arrow[dr, dash] & & Q_2 \arrow[dl, dash] \\
R & & P &
\end{tikzcd}
$$

Lemma 3.22. Let $f : R \to S$ be any ring homomorphism and $P \in \operatorname{Spec} R$. TFAE:

1. $P^{ec} = f^{-1}(f(P)S) = P$, and
2. $\exists Q \in \operatorname{Spec} S$ such that $Q^c = P$. That is, a prime lies over P.

Note that the above is a general fact, no assumptions of integral extensions.

Theorem 3.23 (Going down theorem)**.** Let R be a <u>normal</u> domain, S an <u>integral</u> domain and $R \subset S$ be an integral extension.

Given $P_0, P_1 \in \operatorname{Spec} R$ with $P_0 \supset P_1$ and a prime $Q_0 \in \operatorname{Spec} S$ lying over P_0, there exists a prime $Q_1 \in \operatorname{Spec} S$ lying over P_1 with $Q_0 \supset Q_1$.

$$
\begin{tikzcd}
S \arrow[d, dash, "\text{int}"'] & \mathfrak{q}_1 \arrow[d, dash] & \supset & \exists \mathfrak{q}_2 \arrow[d, dash, dotted] \\
R & \mathfrak{p}_1 & \supset & \mathfrak{p}_2
\end{tikzcd}
$$

In fact, inductively, we see that any chain above can be "completed."

$$
\begin{tikzcd}
S \arrow[d, dash, "\text{int}"'] & \mathfrak{q}_1 \arrow[d, dash] & \supset & \mathfrak{q}_2 \arrow[d, dash] & \supset & \cdots & \supset & \mathfrak{q}_m \arrow[d, dash] & \supset & \exists \mathfrak{q}_{m+1} \arrow[d, dash, dashed] & \supset & \cdots & \supset & \exists \mathfrak{q}_n \arrow[d, dash, dashed] \\
R & \mathfrak{p}_1 & \supset & \mathfrak{p}_2 & \supset & \cdots & \supset & \mathfrak{p}_m & \supset & \mathfrak{p}_{m+1} & \supset & \cdots & \supset & \mathfrak{p}_n
\end{tikzcd}
$$

Theorem 3.24. Let R be a <u>Noetherian</u> normal domain with quotient field K. Let $K \subset L$ be a <u>separable</u> extension. Then, $\overline{R}^L$ is a finite R-module. In particular, it is a Noetherian ring.

Lecture 4. Dimension Theory of Affine Algebra over Fields

Lemma 4.1 (Artin-Tate Lemma)**.** Let $R \subset S \subset T$ be rings. Suppose

1. R is Noetherian,
2. T is a finitely generated S module,
3. T is a finitely generated R algebra.

$$\begin{array}{c} R[t_1, \ldots, t_s] = T = St'_1 + \cdots + St'_k \\ | \\ S \\ | \\ R \end{array}$$

Then, S is a finitely generated R-algebra. In other words, there exist $s_1, \ldots, s_n \in S$ such that $S = R[s_1, \ldots, s_n]$.
In particular, S is Noetherian.

Definition 4.2. Let k be a field. An affine k-algebra is a ring of the form $R = \mathsf{k}[x_1, \ldots, x_n]/I$ for some ideal $I \trianglelefteq \mathsf{k}[x_1, \ldots, x_n]$.

Lemma 4.3 (Zariski)**.** Let k be any field and $R = \mathsf{k}[x_1, \ldots, x_n]/I$ be an affine k-algebra which is also a field. (That is, I is maximal.)
Then, R is an algebraic extension of k.

Corollary 4.4. Let $\varphi : R \to S$ be a ring homomorphism, where R and S are affine k-algebras. Let $\mathfrak{m} \in \operatorname{mSpec}(S)$. Then, $\varphi^{-1}(\mathfrak{m}) \in \operatorname{mSpec}(R)$.

(We had used the fact that if we have an algebraic extension $K \subset F$ of fields and an integral domain R such that $K \subset R \subset F$, then R is a field.)

Theorem 4.5 (Weak Nullstellensatz)**.** If k is algebraically closed, then maximal ideals $\mathfrak{m} \in \operatorname{mSpec} \mathsf{k}[x_1, \ldots, x_n]$ are precisely those of the form $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$ for some $(a_1, \ldots, a_n) \in \mathsf{k}^n$.

Corollary 4.6 (Criterion for solvability)**.** Let $p_1(x_1,\dots,x_n),\dots,p_s(x_1,\dots,x_n)$ be polynomials in $\mathsf{k}[x_1,\dots,x_n]$. Then, the polynomials have a common solution iff the ideal generated by them is not the whole ring.

Remark 4.7. In fact, one need not assume $s<\infty$ in the above.

Definition 4.8. Given a field k, $\mathbb{A}^n_{\mathsf{k}}$ denotes the affine n-space over k. It is simply the set k^n without any vector space structure.

Given any ideal $I \trianglelefteq \mathsf{k}[x_1,\dots,x_n]$, we define the zero set of I as

$$\mathcal{Z}(I)=\{\underline{a}\in\mathbb{A}^n_{\mathsf{k}} : f(\underline{a})=0 \text{ for all } f\in I\}\subset \mathbb{A}^n_{\mathsf{k}}.$$

A subset of $\mathbb{A}^n_{\mathsf{k}}$ which is the zero set of some ideal is called an algebraic set.

Given an algebraic set $X\subset\mathbb{A}^n_{\mathsf{k}}$, we define the ideal of X as

$$\mathcal{I}(X)=\{f\in\mathsf{k}[x_1,\dots,x_n] : f(x)=0 \text{ for all } x\in X\}\subset \mathsf{k}[x_1,\dots,x_n].$$

Remark 4.9. An ideal of an algebraic set is always a radical ideal.

Theorem 4.10 (Strong Nullstellensatz)**.** If k is algebraically closed and $I\trianglelefteq\mathsf{k}[x_1,\dots,x_n]=S$ an ideal, then $\mathcal{I}(\mathcal{Z}(I))=\sqrt{I}$.

In particular, there is a bijection

$$\{\text{radical ideals in } S\}\leftrightarrow\{\text{algebraic subsets in } \mathbb{A}^n_{\mathsf{k}}\}.$$

Definition 4.11. Given a polynomial $f\in\mathsf{k}[x_1,\dots,x_n]$, we can write

$$f=\sum_{\alpha\in(\mathbb{N}\cup\{0\})^n} a_\alpha x^\alpha.$$

If $a_\alpha\neq 0$, we say that x_α is a term of f.

Writing $\alpha=(\alpha_1,\dots,\alpha_n)$, $|\alpha|$ denotes the maximum of $\alpha_1,\dots,\alpha_n$.

Proposition 4.12. Let k be any field. Let $f \in S = \mathsf{k}[x_1, \dots, x_n]$ be a non-constant polynomial. Let

$$N > \max\{|\alpha| : \alpha \in (\mathbb{N} \cup \{0\})^n,\ x^\alpha \text{ is a term of } f\}.$$

Without loss of generality, we may assume that x_n appears non-trivially in some term of f. Define the map $\Phi : S \to S$ by identity on k and

$$x_i \mapsto \begin{cases} x_i - x_n^{N^i} & i \neq n, \\ x_n & i = n. \end{cases}$$

Then, Φ is an automorphism such that $\Phi(f)$ is monic in x_n, up to a constant. That is,

$$\Phi(f) = cx_n^r + g_1 x_n^{r-1} + \cdots + g_n,$$

where $0 \neq c \in \mathsf{k}$ and $g_1, \dots, g_n \in \mathsf{k}[x_1, \dots, x_{n-1}]$.

Theorem 4.13 (Noetherian Normalisation Lemma)**.** Let $R = \mathsf{k}[\theta_1, \dots, \theta_n]$ be an affine k-algebra. Then, there exist algebraically independent elements $z_1, \dots, z_d \in R$ such that $\mathsf{k}[x_1, \dots, x_n] \subset R$ is an integral extension.

$$\begin{array}{c} R \\ \Big| \text{integral} \\ \mathsf{k}[z_1, \dots, z_d] = S. \end{array}$$

In particular, R is a finite S module.

Corollary 4.14. Let R be an affine k-algebra and $I \trianglelefteq R$ an ideal. Then

$$\sqrt{I} = \bigcap_{\mathfrak{m} : I \subset \mathfrak{m} \in \mathrm{mSpec}(R)} \mathfrak{m}.$$

In particular, $\mathcal{N}(R) = \mathcal{J}(R)$.

Definition 4.15. A saturated chain of prime ideals is a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

of prime ideals such that no prime ideal can be inserted strictly in between anywhere above. (In other words, there exists no $i \in \{0, \dots, n-1\}$ and no $\mathfrak{q} \in \mathrm{Spec}(R)$ such that $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i+1}$.)

The length of the above chain is n. The dimension of R is defined as

$$\dim(R) = \sup\{n : \exists \text{ a saturated chain of length } n\}.$$

$\dim(R)$ may be ∞ even if R is Noetherian.

Definition 4.16. Given a prime ideal $\mathfrak{p} \trianglelefteq R$, the height of $\mathfrak{p}$ is defined as

$$\operatorname{height}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}).$$

Example 4.17. Here are some examples.

1. If R is Artinian, then $\dim(R) = 0$. In particular, $\dim(\mathsf{k}) = 0$.
2. $\dim(\mathbb{Z}) = 1$.
3. $\dim(\mathsf{k}[X]) = 1$.
4. In general, if R is a PID and not a field, then $\dim(R) = 1$.

Proposition 4.18. Let $R \subset S$ be an integral extension of rings. Then,

1. $\dim(R) = \dim(S)$.
2. If $I \triangleleft S$ is a proper ideal, then $\dim(S/I) = \dim(R/I \cap R)$.
3. Suppose S is integral and R normal. Let $Q \in \operatorname{Spec}(S)$. Then, $\dim(S_Q) = \dim(R_{Q \cap R})$.

Theorem 4.19. Let R be an affine algebra over a field k. Let $z_1, \ldots, z_d \in R$ be such that $S = \mathsf{k}[z_1, \ldots, z_d] \subset R$ is an integral extension. (Exists by NNL.)
Then,

1. $\dim(R) = d = \dim(\mathsf{k}[z_1, \ldots, z_d])$.
2. Any maximal saturated chain of prime ideals in R has length d.

Remark 4.20. The above shows that the d in Noetherian Normalisation Lemma is determined uniquely. Moreover, it shows that the dimension of polynomial ring in d variables over a field is d.