Contents

Syllabus 1

0.1. course 1

0.2. instructor 1

0.3. topics covered 1

0.4. lecture format 1

0.5. books 1

0.6. prerequisites 1

1. Ideals 2

1.1. maximal ideals 2

1.2. prime ideals 4

1.3. Basic Algebraic Geometry 7

1.4. extension and contraction 9

1.5. unique factorization domains 10

2. Modules 11

2.1. basic concepts 11

2.2. finitely generated modules 11

2.3. exact sequences 13

2.4. kernel and cokernel 14

2.5. tensor product 15

3. Fractions in rings and modules 19

3.1. characterization of \( S^{-1}A \) 19

3.2. localization 20

3.3. localization of modules 20

3.4. review 22

3.5. local properties 22

3.6. extended and contracted ideals in localizations 23

4. Primary decomposition 25

4.1. primary decomposition 25

4.2. associated primes 26

4.3. saturation 27

5. Integral dependence and valuation 29

5.1. integral extensions 29
0.1. course. Math 205b: Commutative Algebra
   MW 2-3:30
   Math Dept Conference Room (on second floor next to math office)

0.2. instructor. Kiyoshi Igusa
   305 Goldsmith
   igusa(at)brandeis.edu
   office hours to be announced
   [webpage for course]

0.3. topics covered. Commutative algebra is mainly the study of
   ideals in commutative rings. It is the basic prerequisite for algebraic
   geometry. This course covers the basic topics of commutative algebra
   using elementary concepts from algebraic geometry for intuition and
   motivation.
   
   (1) prime and primary ideals
   (2) localization
   (3) primary decomposition
   (4) valuations
   (5) completions
   (6) dimension theory

0.4. lecture format. Since each class is an hour and a half, I plan
   to prepare only an hour’s worth of lecture for each class with a list
   of questions for the audience to solve. This means that many of the
   details will be skipped and I plan to fill in the details in the notes.
   Homework problems will be assigned every week but they are op-
   tional.

0.5. books. We will go through the book “Introduction to Commuta-
   tive Algebra” by Atiyah and Macdonald with additional material from:
   
   (1) “Commutative Ring Theory” by Matsumura
   (2) “Commutative Algebra I,II” by Zariski and Samuel
   (3) “Commutative Algebra with a view towards Algebraic Geome-
       try” by Eisenbud
   (4) “Commutative Algebra” by Bourbaki

0.6. prerequisites. This course assumes basic notions of algebra such
   as ideals, modules, tensor product, the basic theorem that integral
   domains are contained in their field of quotients, the structure theorem
   for modules over PID’s. Thus Math 101a should be sufficient. (See my
   Math 101a webpage).
1. Ideals

In this course, all rings $A$ will be commutative with unity $1$. An ideal $a \subseteq A$ is allowed to be all of $A$. So $A/a = 0$ is a ring. (Zero is the only ring in which $1 = 0$.) The ideals we are interested in are the proper ideals $a \subset A$. All homomorphisms of rings are required to take $1$ to $1$. All subrings are required to contain $1$.

We want to discuss the following subsets of ring and how they are expressed in terms of maximal and prime ideals.

1. $D :=$ the set of zero divisors
   \[ D := \{ a \in A \mid \exists b \neq 0, ab = 0 \} \]
   So, $0 \in D$ iff $A \neq 0$.

2. $U :=$ the set (group) of units in $A$.
   \[ U = U(A) := \{ a \in A \mid \exists b \in A, ab = 1 \} \]

3. $n :=$ the set (ideal) of nilpotent elements of $A$.
   \[ n := \{ x \in A \mid \exists n, x^n = 0 \} \]

Exercise: Show that $1 + n \subseteq U$.

1.1. maximal ideals.

**Definition 1.1.** $m$ is a maximal ideal if it is maximal among all proper ideals.

**Proposition 1.2.** $m \subset A$ is maximal iff $A/m$ is a field.

Note: In a field, $1 \neq 0$. So, every field $F$ has exactly two ideals: $0$ and $F$. Also, any element of a ring which is not a unit generates a proper ideal. The proposition follows.

**Theorem 1.3** (A-M 1.3,1.4). Every nonzero ring has maximal ideals and every proper ideal is contained in a maximal ideal.

(by Zorn’s lemma)

**Lemma 1.4** (A-M 1.5). $a \in A$ is a nonunit iff $a$ is contained in some maximal ideal.

**Proposition 1.5.** The set of nonunits of $A$ is equal to the union of all maximal ideals of $A$:
\[ A - U = \bigcup m \]
1.1.1. Jacobson and nil radicals.

**Definition 1.6.** The **Jacobson radical** is defined to be the intersection of all maximal ideals of $A$.

$$\text{rad } A := \bigcap m$$

**Lemma 1.7.** If $x \in \text{rad } A$ then $u + x$ is a unit for all $u \in U$.

**Proof.** Otherwise, $u + x \in m_i \Rightarrow u \in m_i$, a contradiction. \hfill \Box

**Proposition 1.8** (A-M 1.9, variant). Let $a$ be any ideal. Then

$$a \subseteq \text{rad } A \iff 1 + a \subseteq U$$

**Proof.** By the lemma, $a \subseteq \text{rad } A \Rightarrow 1 + a \subseteq U$. Conversely, suppose that $a \not\subseteq m_i$ for some maximal $m_i$. Then $\exists x \in a, x \notin m$ which implies that $x$ is a unit modulo $m$. So, $\exists y \in A$ s.t. $xy \in 1 + m_i$. But then $1 + x(-y) \in m_1$ is not invertible. So, $1 + a \not\subseteq U$. \hfill \Box

If $x \in A$ is nilpotent then $1 + x$ is a unit. Therefore:

**Corollary 1.9.** The set of nilpotent elements of $A$ forms an ideal nilrad $A$ which is contained in the Jacobson radical:

$$\text{nilrad } A \subseteq \text{rad } A$$

**Definition 1.10.** A **local ring** is a ring with a unique maximal ideal. A **semilocal ring** is a nonzero ring with only finitely many maximal ideals.

**Corollary 1.11** (A-M 1.6.ii). Let $m$ be a maximal ideal. Then $1 + m \subseteq U$ iff $A$ is a local ring (iff there are no other maximal ideals.)

**Proof.** By the proposition,

$$1 + m \subseteq U \iff m \subseteq \bigcap m_i \iff \text{no other maximal ideals}$$

\hfill \Box

1.1.2. problems.

1. Let $A[x]$ be the polynomial ring in one generator $x$. Show that $f(x) = a_0 + a_1x + \cdots a_nx^n$ is a unit in $A[x]$ iff $a_0$ is a unit in $A$ and $a_1, \cdots, a_n$ are nilpotent.


3. Show that the only idempotent ($e^2 = e$) contained in $\text{rad } A$ is 0.
1.2. prime ideals.

Definition 1.12. A prime ideal is a proper ideal whose complement is closed under multiplication.

This is equivalent to saying:

\[ ab \in p \iff a \in p \text{ or } b \in p \]

Proposition 1.13. An ideal \( a \) is prime iff \( A/a \) is an integral domain (ring in which \( D = 0 \)). In particular, maximal ideals are prime.

Corollary 1.14. For any ring homomorphism \( f : A \to B \) (which by definition sends 1 to 1), \( f^{-1}(p) \) is prime for any prime \( p \subset B \).

Definition 1.15. The radical of an ideal is defined to be

\[ r(a) := \{ x \in A \mid x^n \in a \text{ for some } n \geq 1 \} \]

Thus, \( r(0) = \text{nilrad } A \).

Exercise 1.16 (A-M 1.13). Prove the following

1. \( r(r(a)) = r(a) \)
2. \( r(ab) = r(a) \cap r(b) \). Recall that a product of ideals \( ab \) is defined to be the ideal generated by all products \( ab \) where \( a \in a, b \in b \).
3. If \( p \) is prime then \( r(p^n) = p \).

Theorem 1.17 (A-M 1.8). The nilradical is the intersection of all prime ideals of \( A \):

\[ r(0) = \text{nilrad } A = \bigcap p \]

Corollary 1.18 (A-M 1.14). The radical of an ideal \( a \) is equal to the intersection all primes containing \( a \):

\[ r(a) = \bigcap_{p \supseteq a} p \]

The proof of this well-known theorem uses properties of unions of prime ideals.

1.2.1. unions of prime ideals. The question is: Which sets are unions of prime ideals?

Definition 1.19. A multiplicative set in \( A \) is a subset \( S \subset A \) which contains 1, does not contain 0 and is closed under multiplication.

For example, the complement of a prime ideal is a multiplicative set.

Lemma 1.20. Let \( S \) be a multiplicative set and let \( a \) be an ideal which is disjoint from \( S \) and maximal with this property. Then \( a \) is prime.
Theorem 1.21. Let $X$ be a nonempty proper subset of $A$. Then $X$ is a union of prime ideals if and only if it satisfies the following condition.

\[(1.1) \quad ab \in X \iff \text{either } a \in X \text{ or } b \in X.\]

Furthermore, any maximal $a \subseteq X$ is prime.

Example 1.22 (A-M exercise 1.14). The set $D$ of zero divisors of $A$ is a union of prime ideals.

Let’s prove the theorem first, assuming the lemma.

Proof of Theorem 1.21. It is clear that any union of primes satisfies condition (1.1). Conversely, suppose that $X$ satisfies (1.1). Then in particular, the complement of $X$ is a multiplicative set. Take any $x \in X$. Then $(x) \subseteq X$. Let $(x) \subseteq a \subseteq X$ where $a$ is maximal with this property. Then $a$ is prime by the lemma. So, $X$ is the union of the prime ideals contained in $X$. □

The proof of the lemma uses the notation:

\[(a : B) := \{x \in A \mid xB \subseteq a\}\]

for any ideal $a$ and subset $B$. This is an ideal which contains $a$.

Exercise 1.23 (I-M 1.12(iii)). Show that

\[((a : b) : c) = (a : bc) = ((a : c) : b)\]

Proof of Lemma 1.20. Suppose that $a \subseteq A - S$ is maximal among the ideals disjoint from $S$. Suppose that $bc \in a$ and $b \notin a$. Then we want to show that $c \in a$. Certainly, $c \in (a : b)$ and $a \subseteq (a : b)$. So, it suffices to prove the following:

Claim: $(a : b)$ is disjoint from $S$.

By maximality of $a$ this would imply that $c \in (a : b) = a$. To prove this claim, take any $x \in (a : b)$. Then $(a : x) \supsetneq a$ since it contains $b \notin a$. So, by maximality of $a$, $S \cap (a : x)$ is nonempty. Say $s \in S \cap (a : x)$. Then $sx \in a$ is disjoint from $S$. So, $x \notin S$ as claimed. □

Proof of Theorem 1.17. It is clear that any nilpotent element of $A$ is contained in every prime ideal. Conversely, suppose that $f \in A$ is not nilpotent. Then $S = \{1, f, f^2, \cdots\}$ is a multiplicative set and $0$ is an ideal disjoint from $S$. Take a ideal $a$ disjoint from $S$ and maximal with this property. Then $a$ is prime by the lemma. So, $f$ is not in $\bigcap p$. □
1.2.2. **prime avoidance.** This is a very important lemma about finite unions of primes.

**Proposition 1.24** (A-M 1.11.i). Suppose that \( X = \bigcup_{i=1}^{n} p_i \) is a finite union of primes. Let \( a \subseteq X \). Then \( a \subseteq p_i \) for some \( i \).

**Proof.** Suppose that \( a \) is not contained in any of the ideals \( p_1, \ldots, p_n \). Then we will show by induction on \( n \) that \( a \) contains an element which is not in any of the \( p_i \).

The statement is trivial for \( n = 1 \) so suppose \( n = 2 \). Then \( a \) contains an element \( a \notin p_1 \) and another element \( b \notin p_2 \). We may assume that \( a \in p_2 \) and \( b \in p_1 \). Then \( a + b \in a \) is not in \( p_1 \cup p_2 \) as claimed.

Suppose that \( n \geq 3 \) and the statement holds for \( n - 1 \). Then for each \( i \), we can assume that \( a \not\subseteq \bigcup_{j \neq i} p_j \) (otherwise \( a \subseteq p_j \)). So, \( a \) contains an element \( a_i \) which is not in \( p_j \) for any \( j \neq i \) and we may assume that \( a_i \in p_i \). Since \( p_n \) is prime, the product \( a_1 \cdots a_{n-1} \) is also not an element of \( p_n \). But it is an element of \( p_1 p_2 \cdots p_{n-1} \). Therefore \( a_1 \cdots a_{n-1} + a_n \) is an element of \( a \) which is not contained in any \( p_i \). \( \square \)

The proof only assumes that \( p_3, p_4, \cdots \) are prime and \( p_1, p_2 \) are just assumed to be ideals.

The other version of prime avoidance is easy.

**Proposition 1.25** (A-M 1.11.ii). If a prime ideal \( p \) contains a finite intersection of ideals \( \bigcap_{i=1}^{n} a_i \), then it contains one of the ideals \( a_i \).

**Exercise 1.26.**

1. Use Zorn’s lemma to show that any nonzero ring has minimal prime ideals.

2. Show that the prime ideals in a product of rings \( A_1 \times A_2 \times \cdots \times A_n \) have the form \( A_1 \times \cdots \times A_{i-1} \times p \times A_{i+1} \times \cdots \times A_n \) where \( p \) is prime. (Recall that in a product of rings, addition and multiplication are coordinate-wise. For example \((a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)\)

**Definition 1.27.** The **annihilator** of an ideal \( a \) is defined to be:

\[
\text{Ann}(a) := (0 : a)
\]

**Exercise 1.28** (A-M 1.15).

\[
D = \bigcup_{x \neq 0} \text{Ann}(x) = \bigcup_{x \neq 0} \text{r(Ann}(x))
\]
1.3. Basic Algebraic Geometry. I will use exercises 15, 17, 21 from the book and other example from other books to review basic algebraic geometry.

Definition 1.29. For any ring \( A \) let \( \text{Spec}(A) \) denote the set of prime ideals of \( A \).

1.3.1. Zariski topology. If \( E \) is any subset of \( A \) let \( V(E) \) denote the set of all prime ideals \( p \) which contain \( E \):

\[
V(E) = \{ p \in \text{Spec}(A) \mid E \subseteq p \}
\]

This function has the property that it reverses inclusion: \( V(E) \supset V(F) \) if \( E \subseteq F \) and \( V(E) = V(a) = V(r(a)) \) if \( a = (E) \) the ideal generated by \( E \). In particular, \( V(x) = V((x)) \) for any \( x \in A \).

Exercise 1.30.
1. \( V(0) = \text{Spec}(A) \)
2. \( V(1) = \emptyset \)
3. \( V(\bigcup E_i) = \bigcap V(E_i) \)
4. \( V(a) \cup V(b) = V(a \cap b) = V(ab) \)

This exercise shows that the collection of subsets \( \{ V(E) \} \) of \( \text{Spec}(A) \) are the closed sets in a topology on \( \text{Spec}(A) \) which is called the Zariski topology. The closed points in \( \text{Spec}(A) \) are the maximal ideals.

For homework, please do: Exercises 17 and 21. They are not hard but we don’t have time to do them in class.

1.3.2. examples. I will take the ring \( A = \mathbb{C}[x, y] \) but I will draw \( \mathbb{R}[x, y] \). The ideal \((x-a, y-b)\) where \( a, b \in \mathbb{C} \) are maximal and we will see later that they are the only maximal ideals since \( \mathbb{C} \) is algebraically closed. So, the closed point in \( \text{Spec} \mathbb{C}[x, y] \) correspond to the points \((a, b)\) in the \( xy \)-plane.

The key observation is:

Proposition 1.31. The point \((a, b)\) is in the zero set of the polynomials \( f_i \in \mathbb{C}[x, y] \) iff

\[
(x-a, y-b) \in \text{Spec} \{ f_i \}
\]

Example 1.32. The prime ideal \((x)\) corresponds to the \( y \) axis. Or more precisely:

\[
V(x) = V((x)) = \{(x), (x, y-b) \mid b \in \mathbb{C}\}
\]

The closed set \( V(x) \) consists of the closed points on the \( y \)-axis and the “generic point” \((x) \in \text{Spec} \mathbb{C}[x, y] \).
Example 1.33. The ideal $a = (xy - x^3)$ is not prime. It is the intersection (and product) of two prime ideals:

$$a = (xy - x^3) = (x)(y - x^2) = (x) \cap (y - x^2)$$

This means that:

$$V(xy - x^3) = V(x) \cup V(y - x^2)$$

This is the union of the y-axis and the parabola $y = x^2$. The fact that the set of zeros of $xy - x^3$ is a union of two sets indicates that it is not prime.

A closed subset of any topological space is called **irreducible** if it is not the union of two proper closed subsets.

**Proposition 1.34.** If $p$ is prime then $V(p)$ is irreducible.

But the converse is not true since $V(p^2) = V(p)$ is irreducible but $p^2$ is not in general prime.

Example 1.35.

$$a = (y^2 - x^2y) = (y)(y - x^2) = (y) \cap (y - x^2)$$

This means that:

$$V(y^2 - x^2y) = V(y) \cup V(y - x^2)$$

This leads to the following questions (which will lead us back to the text).

1. When does $ab = a \cap b$?
2. Can we tell algebraically that the two curves intersect transversely in the first example and tangentially in the second example?
3. What happens if the field is not algebraically closed?

1.3.3. **coprime ideals.**

**Definition 1.36.** Two ideals $a, b$ are called **coprime** if $a + b = A$. Equivalently, $a + b = 1$ for some $a \in a, b \in b$.

**Proposition 1.37.** If $a, b$ are coprime then $ab = a \cap b$.

**Exercise 1.38.** Give an example of two prime ideals $a, b$ in $K[x, y]$ which are coprime and draw the sets $V(a), V(b)$.

**Proposition 1.39** (A-M 1.10.i). $a$ and $b$ are coprime iff $V(a) \cap V(b) = \emptyset$. 

So, the prime ideals in the examples are not coprime. However, if we look at \( p_1, p_2 \) in the two examples we see that, in Example 1.33, \((x) + (y - x^2) = (x, y)\)

is a maximal ideal corresponding to the point \((0, 0)\). In Example 1.35 \((y) + (y - x^2) = (x^2, y)\)

is not maximal, reflecting the fact that the curves are tangent to each other.

**Proposition 1.40** (A-M 1.10.ii). Let \( a_1, a_2, \ldots, a_n \) be ideals and let \( p : A \to \prod A/a_i \) be the homomorphism whose \( i \)-coordinate is the quotient map \( A \to A/a_i \). Then \( p \) is surjective iff the ideals \( a_i \) are pairwise coprime.

1.4. **extension and contraction.**

**Example 1.41.** Take the inclusion map \( f : \mathbb{R}[x, y] \to \mathbb{C}[x, y] \). Then \((x^2 + y^2)\) is prime in \( \mathbb{R}[x, y] \) but \((x^2 + y^2) = (x + iy)(x - iy)\) in \( \mathbb{C}[x, y] \).

So \( V(x^2 + y^2) = V(x + iy) \cup V(x - iy) \)

**Definition 1.42.** Let \( f : A \to B \) be a ring homomorphism. Then for any ideal \( a \) in \( A \) the ideal in \( B \) generated by the image of \( a \) is called the **extension** of \( a \):

\[
a^e := Bf(a) = \left\{ \sum b_i f(a_i) \mid a_i \in a, b_i \in B \right\}
\]

and for any ideal \( b \) in \( B \) its inverse image in \( A \) is an ideal called the **contraction** of \( b \):

\[
b^c = f^{-1}(b)
\]

If \( b \) is prime then the contraction \( b^c = f^{-1}(b) \) is prime. But the example above shows that extension of a prime ideal may not be prime. The example is the book is: \( f : \mathbb{Z} \to \mathbb{Z}[i] \). The extension of the prime ideal \((5)\) is

\[
(5)^e = (2 + i) \cap (2 - i)
\]

If \( f : A \to B \) is surjective, then \( b \subset B \) is prime iff \( b^c \) is prime.

**Proposition 1.43** (A-M 1.17).

1. \( a \subseteq a^{ce}, b \supseteq b^{ce} \)
2. \( a^e = a^{ece} \)
3. \( b^c = b^{ec} \)
4. Let \( C = \{b^c\} = \text{set of contracted ideals} \) and \( E = \{a^e\} = \text{set of extended ideals} \). Then there is a bijection \( C \leftrightarrow E \) given by \( a \mapsto a^e \) and \( b^c \mapsto b \).
1.5. **unique factorization domains.** This is a quick review of UFDs expanding on the comment I made in class about prime and irreducible elements.

**Definition 1.44.** An element \( p \in A \) which is not a unit is called *irreducible* if it is not the product of two nonunits. An element \( p \in A \) is called *prime* if the ideal \((p)\) is prime.

Any prime element is irreducible. However, the converse is not true. An example is given by \( A = \mathbb{Z}[\sqrt{-5}] \). In this ring 2 is irreducible but not prime since \( 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in (2) \) but \( 1 \pm \sqrt{-5} \notin (2) \).

In class I used the contrapositive: If an element \( x \) is not irreducible then \((x)\) is not a prime ideal.

**Exercise 1.45.** Show: If an element of \( A \) can be written as a product of prime elements, then that expression is unique up to reordering and multiplication of each prime element by a unit.

This leads to the definition: \( A \) is a UFD if every nonunit is a product of prime elements.

**Exercise 1.46.** Show that a ring is a UFD iff every irreducible element is prime and any nonempty collection of principal ideals contains a maximal element (the ACC).
2. Modules

2.1. basic concepts. One way to define a module over a ring $A$ is to say that it is an additive group $M$ together with a ring homomorphism $A \to E(M)$

Here $E(M)$ is the ring of all endomorphisms of the additive group $M$. If $M, N$ are $A$ modules then $\text{Hom}(M, N) = \text{the set of all } A\text{-module homomorphisms } f : M \to N$ is also an $A$ module with addition given pointwise: $(f + g)(x) = f(x) + g(x)$ and the action of $A$ given by $(af)(x) = a(f(x)) = f(ax)$

for all $a \in A, x \in M$.

In commutative algebra we are very interested in associating ideals to modules and vice versa. If $\mathfrak{a}$ is an ideal in $A$ then both $\mathfrak{a}$ and $A/\mathfrak{a}$ are module over $A$. For any element $x \in M$ we have the annihilator of $x$

$$\text{Ann}(x) = (0 : x) = \{a \in A | ax = 0\}$$

This is an ideal in $A$ with the property that $A/\text{Ann}(x)$ is isomorphic to the submodule $Ax$ of $M$ generated by $x$. The annihilator of the module is the intersection of annihilators of its elements:

$$\text{Ann}(M) = (0 : M) = \cap_{x \in M} \text{Ann}(x)$$

Here we use the fraction notation: $(X : Y) = \{a \in A | aY \subseteq X\}$. This is an ideal if $X$ is a submodule of $M$ and $Y \subseteq M$ is any subset.

$M$ is called a faithful $A$-module if $\text{Ann}(M) = 0$. Thus $M$ is a faithful $\overline{A}$-module where

$$\overline{A} = A/\text{Ann}(M)$$

Is $M/\mathfrak{a}M$ a faithful $A/\mathfrak{a}$-module?

Exercise 2.1 (A-M 2.2.ii). If $N, P$ are submodules of $M$ then show that

$$(N : P) = \text{Ann}\left(\frac{N + P}{N}\right)$$

2.2. finitely generated modules. If $x_i \in M$ then $\sum x_i$ denotes the submodule of $M$ generated by the $x_i$. The notation reflects the fact that elements can be written (not uniquely) in the form $\sum a_i x_i$ where $a_i \in A$.

$M$ is finitely generated if $M = \sum_{i=1}^{n} Ax_i$ for $x_1, \cdots, x_n \in M$.

Proposition 2.2 (A-M 2.3). $M$ is finitely generated iff $M$ is a quotient of $A^n$ for some finite $n$. 
If \(\varphi : M \to M\) is an endomorphism of \(M\) then we get a ring homomorphism

\[ A[x] \to \text{End}(M) \]

sending \(f(x) = \sum a_i x^i\) to the endomorphism \(\sum a_i \varphi^i\). Then the image \(\overline{A}[\varphi]\) of this homomorphism is a commutative ring and \(M\) is a module over \(\overline{A}[\varphi]\). \((\overline{A} = A/\text{Ann}(M))\)

**Proposition 2.3** (A-M 2.4: the “determinant trick”). *Let \(M\) be a finitely generated \(A\)-module, \(a \subseteq A\) is an ideal and \(\varphi\) is an endomorphism of \(M\) so that \(\varphi M \subseteq aM\) then there exist \(a_1, \cdots, a_n \in a\) so that*

\[ \varphi^n + a_1 \varphi^{n-1} + a_2 \varphi^{n-2} + \cdots + a_n = 0 \]

*as elements of \(\overline{A}[\varphi] \subseteq \text{End}(M)\).*

**Proof.** Let \(x_1, \cdots, x_n\) be generators for \(M\). Then \(aM = \sum a x_i\). So, for each \(i\), \(\varphi(x_i) = \sum a_{ij} x_j\) for some \(a_{ij} \in a\). This implies that the column vector with entries \(x_1, \cdots, x_n\) is annihilated by the matrix \(\varphi I_n - (a_{ij})\)

\[ (\varphi \delta_{ij} - (a_{ij}))(x_j) = 0 \]

If we view the matrix \(B = \varphi I_n - (a_{ij})\) as a matrix with coefficients in the commutative ring \(\overline{A}[\varphi]\) then we see that its determinant must annihilate all of the \(x_j\). This is because there is another matrix \(adB\) with coefficients in the same ring so that \(adB\) times \(B\) is the diagonal matrix \((\det B) I_n\):

\[ adBB(x_j) = 0 = (\det B) I_n(x_j) = (\det B)(x_j) \]

Since \(\det B\) annihilates all the generators of \(M\), it is the zero element of the endomorphism ring. So, \(\det B = \varphi^n + a_1 \varphi^{n-1} + \cdots = 0\) as claimed. \(\square\)

**Corollary 2.4** (A-M 2.5). *If \(M\) is finitely generated and \(aM = M\) then there exists an \(a \in a\) so that \((1 + a)M = 0\).*

**Proof.** Let \(\varphi : M \to M\) be the identity. Then the proposition says that

\[ 1 + a_1 + \cdots + a_n = 0 \in \text{End}(M) \]

where \(a_i \in a\). So \(a = \sum a_i\) is the required element of \(a\). \(\square\)

Note that if \(a\) is contained in the Jacobson radical \(\text{rad}(A)\) then \(1 + a\) is a unit. So \((1 + a)M = 0\) iff \(M = 0\). This proves:

**Theorem 2.5** (A-M 2.6: Nakayama’s Lemma). *If \(a \subseteq \text{rad}(A)\) and \(M = aM\) then \(M = 0\) (assuming \(M\) is finitely generated).*

This is also very easy to prove by induction on the number of generators.
Corollary 2.6 (A-M 2.7). Suppose $M$ is finitely generated and $N$ is a submodule of $M$. Let $a \subseteq \text{rad}(A)$ and suppose that $M = aM + N$. Then $M = N$.

Proposition 2.7 (A-M 2.8). Suppose that $A$ is a local ring with unique maximal ideal $m$ and $M$ is a f.g. $A$-module. Then a subset of $M$ generates $M$ iff its image in $M/mM$ generates this vector space over the field $A/m$.

Proposition 2.8. Suppose that $M$ is f.g. and $\varphi : M \rightarrow M$ is a surjective endomorphism. Then $\varphi$ is also injective.

Proof. Consider $M$ as a module over $B = \overline{A}[\varphi]$. In this ring the principal ideal $(\varphi) = B\varphi$ has the property that $(\varphi)M = M$. So, there exists an $f \in (\varphi)$ so that $(1 + f)M = 0$. Let $x \in \ker \varphi$ then $(\varphi)$ annihilates $x$. So, $f(x) = 0$ and $0 = (1 + f)(x) = x$. So, $\ker \varphi = 0$. □

2.3. exact sequences.

Proposition 2.9 (A-M 2.9 Hom is left exact). If

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$$

is exact then so is the induced sequence

$$0 \rightarrow \text{Hom}(M'', N) \xrightarrow{\beta^*} \text{Hom}(M, N) \xrightarrow{\alpha^*} \text{Hom}(M', N)$$

If

$$0 \rightarrow N' \xrightarrow{\gamma} N \xrightarrow{\delta} N''$$

is exact then so is

$$0 \rightarrow \text{Hom}(M, N') \xrightarrow{\gamma^*} \text{Hom}(M, N) \xrightarrow{\delta^*} \text{Hom}(M, N')$$

Proposition 2.10. If

$$M' \rightarrow M \rightarrow M'' \rightarrow 0$$

is exact and $M', M''$ are f.g. then so is $M$.

Corollary 2.11. If

$$0 \rightarrow X \rightarrow Y \rightarrow M \rightarrow 0$$

is an exact sequence of $A$-modules and $Y$ is f.g. and $M$ is finitely presented, then $X$ is finitely generated.

$M$ is finitely presented if it is finitely generated and there is an epimorphism $f : A^n \rightarrow M$ whose kernel is also finitely generated.
2.4. **kernel and cokernel.** In class I went over the categorical definition of kernel and cokernel and used it to explain the left exactness of Hom.

**Definition 2.12.** Let $f : M' \to M$ be a homomorphism of $A$-modules and let $\beta : M \to C$ to a homomorphism with the following two properties

1. The composition $\beta \circ f : M' \to C$ is zero.
2. For any other module $C'$ and homomorphism $\beta' : M \to C'$ with the property that $\beta' \circ f = 0$ there exists a unique homomorphism $g : C \to C'$ so that $\beta' - g \circ \beta$

Then the pair $(\beta, C)$ is the cokernel of the map $f$. (Normally we say $C$ together with the map $\beta$.) Since this is a universal property, $C$ and $(\beta, C)$ are uniquely determined up to isomorphism assuming that they exist.

In Proposition 2.9 $(\beta, M'')$ is the cokernel of $\alpha$. Therefore, if $g \in \text{Hom}(M, N)$ and $\alpha^\#(g) = g \circ \alpha = 0$, then, by definition of the cokernel, there exists a unique $h : M'' \to N$ so that $g = h \circ \beta = \beta^\#(h)$. Therefore, $\ker \alpha^\# = \text{im} \beta^\#$. 

The definition of kernel and proof of the second part of Proposition 2.9 are analogous.
2.5. tensor product.

2.5.1. definition and basic properties. The best description of the tensor product is given by the universal property. But, we need to have a concrete description so that we can distinguish between equal and isomorphic modules.

Given modules $M, N, P$ a mapping $f : M \times N \to P$ is called bilinear if for all $x \in M$ and $y \in N$ the mappings

\[ f(x, -) : N \to P \]
\[ f(-, y) : M \to P \]

are homomorphisms of $A$-modules.

**Proposition 2.13 (A-M 2.12).** For any two modules $M, N$ there is a module $T$ and a bilinear mapping $f : M \times N \to T$ which has the property that, for any other bilinear mapping $g : M \times N \to P$ there is a unique homomorphism $h : T \to P$ so that $g = h \circ f$.

\[
\begin{array}{ccc}
X \times Y & \overset{f}{\longrightarrow} & T \\
\downarrow g & & \downarrow \exists h \\
& P &
\end{array}
\]

Furthermore, $T$ is unique up to isomorphism.

The uniqueness of $T$ up to isomorphism is clear. Existence is given by the following construction.

**Definition 2.14.** If $M, N$ are modules, then let $M \otimes N$ be the $A$-module constructed as follows. Take the free module on the set $M \times N$. This is $C = A^{(M \times N)}$. Let $D$ be the submodule of $C$ generated by all elements of the form

\[(2.1) \quad (ax + by, z) - a(x, z) - b(y, z)\]
\[(2.2) \quad (x, az + bw) - a(x, z) - b(x, w)\]

for all $x, y \in M$, $z, w \in N$ and $a, b \in A$. Then the quotient $C/D$ is called the tensor product of $M$ and $N$ and denoted by $M \otimes N$. The image of $(x, y) \in M \times N$ in $M \otimes N$ is denoted $x \otimes y$.

**Proof of Proposition 2.13.** The mapping $f : M \times N \to M \otimes N$ given by $f(x, y) = x \otimes y$ is clearly bilinear and any mapping $g : M \times N \to P$ induces a unique mapping $\overline{g} : C \to P$ and $g$ is bilinear iff $D \subseteq \ker \overline{g}$. So, we get an induced map $h : C/D = M \otimes N \to P$. The map is unique since the elements $x \otimes y$ generate $M \otimes N$ and $h$ must send $x \otimes y$ to $f(x, y)$.

\[\square\]
The tensor product has the important functorial property that, given homomorphisms \( f : M \to M' \) and \( g : N \to N' \) there is an induced homomorphism

\[
f \otimes g : M \otimes N \to M' \otimes N'
\]

given by \((f \otimes g)(x \otimes y) = f(x) \otimes g(y)\). (Since \(f(x) \otimes g(y)\) is bilinear in \((x, y)\) we get this induced map.)

**Proposition 2.15.** We have natural isomorphisms

1. \( M \otimes N \cong N \otimes M \).
2. \( M \otimes (N \otimes P) \cong (M \otimes N) \otimes P \)
3. \( (M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P) \).
4. \( A \otimes M \cong M \)

**Natural isomorphism** means that the following diagram commutes (in the first case)

\[
\begin{array}{ccc}
M \otimes N & \xrightarrow{\cong} & N \otimes M \\
\downarrow f \otimes g & & \downarrow g \otimes f \\
M' \otimes N' & \xrightarrow{\cong} & N' \otimes M'
\end{array}
\]

Problem: If \( a, b \) are coprime show that \( A/\mathfrak{a} \otimes A/\mathfrak{b} = 0 \).

2.5.2. **homological properties.** The basic homological properties of tensor product are

1. tensor product is **right exact** and
2. tensor product is **left adjoint** to Hom.

The second property implies that first (and also implies that Hom is left exact). However, I want to start by stating the first property.

**Proposition 2.16** (A-M 2.18). Suppose that \( M' \to_f M \to_g M'' \to 0 \) is an exact sequence of \( A \)-modules and \( N \) is another \( A \)-module. Then

\[
M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0
\]

is exact.

**Proof.** The fact that \( g \otimes 1 : M \otimes N \to M'' \otimes N \) is onto is obvious. However, exactness at the other point is not obvious. What we do is to show that \( M'' \otimes N \) is the cokernel in the diagram. This means that given any module \( P \) and homomorphism \( h : M \otimes N \to P \) so that the composition

\[
M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{h \circ} P
\]

is zero, there is a unique way to factor the map \( h \) through \( M'' \otimes N \).
Lemma 2.17. There is a natural isomorphism
\[ \text{Hom}(M \otimes N, P) \cong \text{Hom}(M, \text{Hom}(N, P)) \]
given by sending \( h : M \otimes N \to P \) to \( \hat{h} \) where \( \hat{h}(x) = h(x \otimes -) : N \to P \) for all \( x \in M \).

Assuming that the lemma is true, we continue the proof of the proposition. First, we claim that \( \hat{h} \circ f = 0 : M' \to M \to \text{Hom}(N, P) \). This is a simple calculation:
\[ \hat{h}(f(x)) = h(f(x) \otimes -) = 0 \]
Therefore \( \hat{h} \) factors uniquely through \( M'' \):

\[
\begin{array}{ccc}
M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \rightarrow & 0 \\
\downarrow{0} & & \downarrow{\hat{h}} & & \downarrow{\exists k} & & \\
\text{Hom}(N, P) & & & & & & \\
\end{array}
\]

Using the lemma again, the induced homomorphism \( M'' \to \text{Hom}(N, P) \) is the adjoint of a unique mapping \( k : M'' \otimes N \to P \) so that \( k \circ g \otimes 1 = 0 \). So, \( (g \otimes 1, M'' \otimes N) \) is the cokernel of \( f \otimes 1 \) as claimed. \( \square \)

Proof of Lemma 2.17. The map going from right to left sends \( f : M \to \text{Hom}(N, P) \) to the map \( \hat{f} : M \otimes N \to P \) given by \( \hat{f}(x \otimes y) = f(x)(y) \).
Since this is bilinear, it induces a map on the tensor product. It is straightforward to check that these two “adjunction maps” are inverse to each other. \( \square \)

Exercise 2.18. (1) Show that \( M/\mathfrak{a}M \cong A/\mathfrak{a} \otimes M \).
(2) If \( M \) is finitely generated and nonzero, then show that there is a maximal ideal \( \mathfrak{m} \) so that \( M/\mathfrak{m}M \neq 0 \).
(3) If \( A^n \cong A^m \) show that \( n = m \). (Remember that \( A/\mathfrak{m} \) is a field.)

2.5.3. change of rings. Tensor product is useful for explaining what is extension of scalars. If \( \varphi : A \to B \) is a ring homomorphism then the restriction of scalars functor is given by taking any \( B \)-module \( M \) and considering the same additive group \( M \) as an \( A \)-module with action of \( a \in A \) given by multiplication by the image of \( a \) in \( B \):
\[ a(x) = \varphi(a)x \]
We call this \( _AM \). In particular \( B \) becomes an \( A \)-module \( _AB \).

The extension of scalars functor takes an \( A \)-module \( M \) and gives a \( B \) module
\[ M_B = B \otimes_A M \]
(When there is more than one ring, it is helpful to put the subscript \( \otimes_A \) to indicate that it is tensor product as \( A \)-modules.) The \( B \)-module structure on \( M_B \) is given by multiplication on the first factor:

\[
    b(c \otimes x) = (bc) \otimes x
\]

More generally, if \( N \) is a \( B \)-module, we can consider \( N \) as an \( A \)-module by restriction of scalars and we can take the tensor product \( N \otimes_A M \). This is a \( B \)-module with action of \( B \) given by multiplication on the first tensor factor.

**Proposition 2.19** (A-M 2.15). If \( M, N \) are \( B \)-modules and \( P \) is an \( A \) module then

\[
    M \otimes_B (N \otimes_A P) \cong (M \otimes_B N) \otimes_A P
\]

**Proposition 2.20** (A-M 2.17). If \( M \) is a f.g. \( A \)-module then \( M_B \) is a f.g. \( B \)-module.

**Proposition 2.21** (A-M 2.16). If \( M \) is a f.g. \( B \)-module and \( B \) is f.g. as an \( A \)-module then \( A_M \) is a f.g. \( A \)-module.

When we have a fixed ring homomorphism \( \varphi : A \to B \) we say that \( B \) is an algebra over \( A \). If \( B \) is finitely generated as an \( A \)-module then we say that \( B \) is a finite \( A \)-algebra. For example \( A[x]/(x^2) \) is a finite algebra over \( A \). \( A[x, y] \) is not a finite algebra but it is finitely generated (by \( x, y \)). An \( A \)-algebra is finitely generated if it is a quotient of a polynomial algebra \( A[x_1, \ldots, x_n] \) over \( A \) in finitely many variables.

2.5.4. flat modules. If \( \otimes N \) is exact then \( N \) is called a flat module. This means that for any short exact sequence \( 0 \to M' \to M \to M'' \to 0 \) we get a short exact sequence

\[
    0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0
\]

**Exercise 2.22.**

(1) \( A \) is flat.

(2) If \( N, N' \) are flat then \( N \oplus N' \) is flat

(3) If \( N, N' \) are flat then \( N \otimes N' \) is flat

(4) If \( N \) is flat then \( \otimes N \) takes long exact sequences to long exact sequences.

(5) If \( N \) is a flat \( A \)-module and \( B \) is an algebra over \( A \) then \( N_B \) is a flat \( B \)-module.
3. Fractions in rings and modules

Atiyah and MacDonald define multiplicative sets to be subsets $S \subseteq A$ of a ring so that $1 \in S$ and $S$ is closed under multiplication. They don’t assume $0 \notin S$ (as in my Def 1.19). So, we will now allow 0 to be in $S$.

(But, if $0 \in S$ then $S^{-1}A = 0$ and $S^{-1}M = 0$)

If $S \subseteq A$ is a multiplicative set then define $S^{-1}A$ to be the ring whose elements are equivalence of pairs $(a, s)$ where $a \in A, s \in S$ with equivalence relation:

$$(a, s) \sim (b, t) \iff atu = bsu \text{ for some } u \in S.$$  

Equivalence classes are written $a/s$ or $a_s$. Letting $(b, t) = (0, 1)$ we get:

$$a_s = 0 \text{ in } S^{-1}A \iff au = 0 \text{ for some } u \in S$$

Putting $a = 1$ we see that $S^{-1}A = 0$ iff $0 \in S$.

Addition and multiplication are given in the usual way by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \frac{b}{t} = \frac{ab}{st}$$

There is a ring homomorphism $f : A \to S^{-1}A$ given by $f(a) = a/1$.

$$f(a) = 0 \iff as = 0 \text{ for some } s \in S.$$  

**Exercise 3.1.** (1) Let $A = \mathbb{Z}, S = \mathbb{Z} - (3), T = 1 + (3)$. Show that $S^{-1}\mathbb{Z} = T^{-1}\mathbb{Z}$.

(2) More generally, show that if $m$ is a maximal ideal, $S = A - m$ and $T = 1 + m$ then $S^{-1}A = T^{-1}A$.

One standard example is when $A$ is an integral domain and $S = A - \{0\}$. Then $S^{-1}A$ is a field called the **field of fractions** of $A$.

3.1. **characterization of $S^{-1}A$.** The ring $S^{-1}A$ is characterized by a universal property which can be stated abstractly and more concretely.

**Proposition 3.2** (A-M 3.1). *If $S \subset A$ is a multiplicative set then $S^{-1}A$ has the following universal property: Given any ring homomorphism $g : A \to B$ so that $g(S) \subseteq U(B)$ then there exists a unique ring homomorphism $h : S^{-1}A \to B$ so that $h \circ f = g$. I.e., the following diagram commutes.*

$$\begin{array}{ccc}
A & \xrightarrow{g} & B \\
\downarrow{f} & & \downarrow{h} \\
S^{-1}A & \xrightarrow{f} & \end{array}$$
This categorical language is not as useful as the concrete interpretation:

**Corollary 3.3** (A-M 3.2). Suppose that \( g : A \to B \) is a ring homomorphism. Then \( B \cong S^{-1}A \) iff it has the following properties.

1. \( s \in S \Rightarrow g(s) \) is a unit in \( B \).
2. \( g(a) = 0 \Rightarrow as = 0 \) for some \( s \in S \).
3. Every element of \( B \) has the form \( g(s)^{-1}g(a) \) for some \( s \in S, a \in A \).

**Proof.** (1) says that \( g \) factors through \( S^{-1}A \). (3) says the induced map \( h : S^{-1}A \to B \) is onto. (2) says that \( h \) is 1-1. \( \square \)

3.2. **localization.** The most important case of this construction is when \( S = A - p \) is the complement of a prime ideal \( p \). But first, we need to do the following easy exercise:

**Exercise 3.4.** For any multiplicative set \( S \) and ideal \( a \) in \( A \) show that

\[
S^{-1}a = \left\{ \frac{a}{s} \mid a \in a, s \in S \right\}
\]

is an ideal in \( S^{-1}A \) equal to the extension \( a^e \).

**Theorem 3.5.** If \( S = A - p \) is the complement of a prime ideal \( p \) then \( S^{-1}A \) is a local ring with unique maximal ideal \( S^{-1}p \).

This local ring is denoted \( A_p = S^{-1}A \) and called the **localization** of \( A \) at \( p \).

3.3. **localization of modules.** If \( M \) is an \( A \)-modules and \( S \subseteq A \) is a multiplicative set then let \( S^{-1}M \) be the set of all equivalence classes of pairs \((x, s) \in M \times S \) where

\[
(x, s) \sim (y, t) \iff xtu = ysu \text{ for some } u \in S.
\]

The equivalence class of \((x, s)\) is written \( x/s \). Taking \((y, t) = (0, 1)\) we get

\[
\frac{x}{s} = 0 \in S^{-1}M \iff xu = 0 \text{ for some } u \in S
\]

Then \( S^{-1}M \) is an \( S^{-1}A \)-module with action of \( S^{-1}A \) given by

\[
\frac{ax}{st} = \frac{ax}{st}
\]

**Exercise 3.6.** If \( M \) is finitely generated then show that \( S^{-1}M = 0 \) iff there exists an \( s \in S \) so that \( sM = 0 \).
In the special case $S = A - p$ where $p$ is prime, we write

$$S^{-1}M = M_p$$

If $f : M \rightarrow N$ is a homomorphism of $A$-modules, we get an induced homomorphism of $S^{-1}A$-modules $S^{-1}f : S^{-1}M \rightarrow S^{-1}N$ given by $S^{-1}f(x/s) = f(x)/s$. We get the following important theorem with an easy proof.

**Theorem 3.7** (A-M 3.3). The functor $S^{-1}$ is exact, i.e. given any exact sequence $M' \rightarrow_f M \rightarrow_g M''$, we get an exact sequence

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

The module $S^{-1}M$ satisfies a universal property similar to the one for $S^{-1}A$. That universal property can be expressed in the following terms.

**Proposition 3.8.** Given an $A$-module $M$ and an $S^{-1}A$-module $N$ we have a natural isomorphism

$$\text{Hom}_A(M, AN) \cong \text{Hom}_{S^{-1}A}(S^{-1}M, N)$$

where $AN$ is $N$ considered as an $A$-module by restriction of scalars.

To see that this is a universal property, look at the following diagram:

$$\begin{array}{ccc}
M & \xrightarrow{g} & N \\
\downarrow{f} & & \downarrow{\cong h} \\
S^{-1}M & & \\
\end{array}$$

Given any $g : M \rightarrow AN$ we get a unique $h : S^{-1}M \rightarrow N$.

**Corollary 3.9** (A-M 3.5). $S^{-1}M \cong S^{-1}A \otimes_A M$.

**Proof.** The adjunction formula

$$\text{Hom}_A(M, AN) \cong \text{Hom}_{S^{-1}A}(S^{-1}A \otimes_A M, N)$$

tells us that $S^{-1}A \otimes_A M$ satisfies the same universal formula! \qed

**Corollary 3.10** (A-M 3.6). $S^{-1}A$ is a flat $A$-module.

**Exercise 3.11.** If $S = 1 + a$ then show that

$$S^{-1}(A/a) = A/a$$
3.4. review. 
\[ \frac{x}{s} = 0 \text{ in } S^{-1}M \iff xu = 0 \text{ for some } u \in S \]
and (Corollary 3.9):
\[ S^{-1}M \cong S^{-1}A \otimes M \]

**Lemma 3.12** (A-M 3.7). \( S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N. \) In particular:
\[ (M \otimes_A N)_p \cong M_p \otimes_{A_p} N_p \]

3.5. **local properties.** A property \( P \) describing a class of rings or modules is called **local** if property \( P \) holds for a ring \( A \) (or module) iff it holds for every localization \( A_p \) at a prime ideal has property \( P \). For example, the property of being equal to 0 is local:

**Proposition 3.13** (A-M 3.8). If \( M \) is an \( A \)-module, the following are equivalent.

1. \( M = 0 \)
2. \( M_p = 0 \) for every prime ideal \( p \) in \( A \)
3. \( M_m = 0 \) for every maximal ideal \( m \) in \( A \).

**Proof.** \((1) \implies (2) \implies (3) \) is clear. So, we just need to show \( \neg(1) \implies \neg(3). \)
If \( x \neq 0 \in M \) consider \( \text{Ann}(x) \subseteq m. \)

Using the exactness of localization, we can easily get:

**Corollary 3.14** (A-M 3.9). Suppose that \( \varphi : M \to N \) is a homomorphism of \( A \)-modules. Then the following are equivalent.

1. \( \varphi \) is a monomorphism.
2. \( \varphi_p : M_p \to N_p \) is a monomorphism for every prime ideal \( p \) in \( A \)
3. \( \varphi_m : M_m \to N_m \) is a monomorphism for every maximal ideal \( m \) in \( A \).

And the same holds with “monomorphism” replace with “epimorphism.”

This, and Lemma 3.12 imply that flatness is a local property:

**Proposition 3.15** (A-M 3.10). If \( M \) is an \( A \)-module, the following are equivalent.

1. \( M \) is flat.
2. \( M_p \) is a flat \( A_p \)-module for every prime ideal \( p \) in \( A \)
3. \( M_m \) is a flat \( A_m \)-module for every maximal ideal \( m \) in \( A \).
3.6. **extended and contracted ideals in localizations.** Recall: for the ring homomorphism \( f : A \to S^{-1}A \) the extension of an ideal \( a \subseteq A \) is given by \( a^e = S^{-1}a \) and the contraction of an ideal \( b \subseteq B \) is, by definition, \( b^e = f^{-1}(b) \). It is clear that the contraction of a prime ideal is prime.

Also, there is always a bijection between the set of contracted ideals \( C = \{ b^e \} = \{ a \subseteq A \mid a = a^e \} \) and the set of extended ideals:

\[
E = \{ a^e \} = \{ b \subseteq B \mid b = b^e \}
\]

**Proposition 3.16 (A-M 3.11).**

(i) Every ideal in \( S^{-1}A \) is an extended ideal.

(ii) If \( a \) is an ideal in \( A \) then

\[
a^e = \bigcup_{s \in S} (a : s)
\]

So, \( a^e = S^{-1}A \) iff \( S \cap a \neq \emptyset \).

(iv) \( p \leftrightarrow p^e \) gives a bijection between the primes in \( A \) disjoint from \( S \) and the primes in \( S^{-1}A \).

**Proof.** (i), (ii) are easy. For (iv): If \( q \) is a prime ideal in \( S^{-1}A \) then \( q^e \) is prime in \( A \) and \( q^e = q \). So, \( q^e \) is disjoint from \( S \) by (ii).

Going the other way, suppose that \( p \) is a prime ideal in \( A \) disjoint from \( S \). In other words, \( S \subseteq T = A - p \). Then,

\[
S^{-1}T = \left\{ \frac{t}{s} \mid t \in T, \ s \in S \right\}
\]

is a multiplicative subset of \( S^{-1}A \) and

\[
S^{-1}A = S^{-1}T \prod S^{-1}p
\]

Therefore \( p^e = S^{-1}p \) is a prime ideal in \( S^{-1}A \). \( \square \)

**Corollary 3.17 (A-M 3.13).** If \( p \subseteq A \) is prime then the prime ideals of \( A_p \) are \( q_p \) where \( q \) is a prime contained in \( p \).

**Exercise 3.18.**

(1) Show that the ring homomorphism \( f : A \to S^{-1}A \) induces an injective mapping:

\[
f^* : \text{Spec}(S^{-1}A) \to \text{Spec}(A)
\]

(2) If \( S = \{1, h, h^2, h^3, \ldots \} \) then \( S^{-1}A \) is denoted \( A_h \) and the image of \( \text{Spec}(A_h) \) in \( \text{Spec}(A) \) is the set

\[
X_h = \{ p \mid h \notin p \}
\]
(3) Show that the mapping in (1) is a homeomorphism onto its image. Recall that the basic open sets in $\text{Spec}(A)$ are the subsets $X_h$ above. (The closed sets are $V(E) = \{ p \mid E \subseteq p \}$.)

**Proposition 3.19 (A-M 3.11(v)).**

1. $S^{-1}(a \cap b) = S^{-1}a \cap S^{-1}b$
2. $S^{-1}(ab) = (S^{-1}a)(S^{-1}b)$
3. $S^{-1}(a + b) = S^{-1}a + S^{-1}b$
4. $S^{-1}(r(a)) = r S^{-1}a$

Putting $a = 0$ in (4) we get:

**Corollary 3.20 (A-M 3.12).** $S^{-1}\text{nilrad } A = \text{nilrad } S^{-1}A$

**Lemma 3.21.** $\text{Ann}(S^{-1}(A/a)) = S^{-1}a$

**Proposition 3.22 (A-M 3.14).** If $M$ is a f.g. $A$-module then

$$\text{Ann}(S^{-1}M) = S^{-1}\text{Ann}(M)$$

Since $(N : P) = \text{Ann} \left( \frac{N + P}{N} \right)$ we get:

**Corollary 3.23 (A-M 3.15).** If $N,P$ are submodules of $M$ and $P$ is f.g. Then

$$S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$$
4. Primary decomposition

This chapter of Atiyah-MacDonald is different from other treatments of primary decomposition because it does not assume that the ring $A$ is Noetherian. So, the definition of an associated prime is different.

Definition 4.1. An ideal $q$ in $A$ is called primary if every zero divisor in $A/q$ is nilpotent. This is equivalent to saying:
\[ xy \in q, x \notin q \Rightarrow y^m \in q \text{ for some } m \geq 1 \]

In other words, $y \in r(q)$.

Note that prime ideals are primary.

Proposition 4.2. $q$ primary implies $r(q)$ is prime.

Proof. If $xy \in r(q)$ then $x^ny^n \in q$ for some $n$. If $x \notin r(q)$ then $x^n \notin q$. So, $(y^n)^m \in q$ which implies $y \in r(q)$. So, $r(q)$ is prime. \[ \square \]

We say that $q$ is $p$-primary if $r(q) = p$.

Proposition 4.3. $p/q$ contains all zero divisors of $A/q$.

4.1. Primary decomposition.

Definition 4.4. A primary decomposition of an ideal $a$ is defined to be an expression of the form:
\[ a = \bigcap_{i=1}^{n} q_i \]

where $q_i$ are primary and $n$ is finite. If $n$ is minimal, this is called a minimal primary decomposition.

Let $p_i = r(q_i)$. The following lemma shows that, in a minimal primary decomposition, the $p_i$ are distinct.

Lemma 4.5. If $q_1, q_2$ are $p$-primary (for the same $p$) then $q_1 \cap q_2$ is also $p$-primary.

Proof. Suppose that $xy \in q_1 \cap q_2$ but $x \notin q_1 \cap q_2$. Then either $x \notin q_1$ or $x \notin q_2$. In either case we get $y \in p$. Then $y^n \in q_1$ and $y^m \in q_2$. So, $y^{nm} \in q_1 \cap q_2$ making this primary. And it is easy to see that the radical is $p$. \[ \square \]

Example 4.6. Here are two examples of primary decompositions.

1. $(12) = (4) \cap (3)$ in $A = \mathbb{Z}$. Here $q_1 = (4) = p_1^2$, $p_1 = (2)$ and $q_2 = p_2 = (3)$.

2. $(x^2, xy) = (x) \cap (x, y)^2$ in $A = k[x, y]$ where $k$ is a field. Here $q_1 = (x) = p_1$ and $q_2 = p_2^2$ with $p_2 = (x, y)$. 

This example is not typical since the primary ideals are powers of prime ideals.

1. \( p^m \) might not be primary.
2. \( q \) being \( p \)-primary does not imply \( q = p^m \).

The second statement is not surprising and it is easy to find examples, e.g., \( p = m = (x,y) \) in \( A = k[x,y] \). There are many ideals \( q \) between \( m \) and \( m^2 \) and they are all \( m \)-primary by Prop. 4.8 below. But the first statement is surprising.

**Example 4.7.** Let \( A = k[x,y,z]/(xy - z^2) \) and let \( x, y, z \in A \) be the images of \( x, y, z \). Then \( p = (\bar{x}, \bar{z}) \) is prime since \( A/p = k[\bar{y}] \) is the polynomial ring in one generator \( \bar{y} \). (No power of \( \bar{y} \) is in \( p \).)

Claim: \( p^2 = (\bar{x}^2, \bar{z}^2, \bar{xz}) \) is not primary.

For the proof, note that \( \bar{x} \bar{y} = \bar{z}^2 \in p^2 \) but \( \bar{x} \notin p^2 \) and \( \bar{y}^m \notin p^2 \) for all \( m \) since \( p^2 \subset p \) which does not contain any power of \( \bar{y} \). So, \( p^2 \) is not primary.

**Proposition 4.8.** If \( r(a) = m \) is maximal then \( a \) is primary. In particular, \( m^n \) is primary.

Note that in the examples I gave the primary ideals which were not prime were powers of maximal ideals.

**Proof.** We have an epimorphism \( A/a \to A/r(a) = A/m \) which is a field. We need to show that every zero divisor \( x \in A/a \) is nilpotent. Suppose not. Then \( x \mapsto \bar{x} \neq 0 \in A/r(a) \). Since this is a field, \( \bar{x} \) is not a zero divisor. So, \( x \) is not a zero divisor. \( \Box \)

4.2. **associated primes.** Before we do the associated primes, we need to review the prime avoidance lemma [1.2.2] which has two forms:

1. If \( a \subseteq \bigcup_{i=1}^n p_i \) then \( a \subseteq p_i \) for some \( i \).
2. If \( p \supseteq \bigcap_{i=1}^n a_i \) then \( p \supseteq a_i \) for some \( i \). And, if \( p = \bigcap a_i \) then \( p = a_i \) for some \( i \).

**Definition 4.9.** Given an \( A \)-module \( M \) an **associated prime**[1] is defined to be a prime ideal of the form \( r(\text{Ann}(x)) \) for some \( x \in M \). Taking \( M = A/a \), the associated primes for \( a \) are those of the form

\[ p = r(a : x) \]

for some \( x \in A \).

**Theorem 4.10.** If \( a = \bigcap q_i \) is a minimal primary decomposition then the prime ideals \( p_i = r(q_i) \) are exactly the associated primes for \( a \).

---

1In the Noetherian case \( p \) is an associated prime if \( p = (a : x) \) for some \( x \in A \).
Proof. We have two sets of prime ideals and we need to show that they are equal. To show that the first set is contained in the second, suppose that \( p \) is an associated prime. Then

\[
p = r(a : x) = r \left( \bigcap q_i : x \right) = r \bigcap (q_i : x) = \bigcap r(q_i : x)
\]

By prime avoidance we have

\[
p = r(q_i : x).
\]

But

\[
(q_i : x) = \{ a \in A | ax \in q_i \}
\]

is a set of zero divisors modulo \( q_i \). So \( q_i \subseteq (q_i : x) \subseteq p_i \). This implies that \( p = p_i \). So, the first set is contained in the second.

To show the converse, take \( p_1 = r(q_1) \). We need to show that \( p_1 = r(a : x) \) for some \( x \in A \). Since \( n \) is minimal, \( a \subset \bigcap_{i=1}^n q_i \). So, there is some \( x \in \bigcap_{i=1}^n q_i \) so that \( x \notin a \) and \( x \notin q_1 \).

Claim: \( r(a : x) = p_1 \).

This is all we have to show. It is clear that \( q_1 \subseteq (a : x) \) since \( x \) is already in all of the other \( q_i \) and multiplying it by any element of \( q_1 \) will put it in \( \bigcap q_i = a \). So, all we have to do is to show that

\[
(a : x) \subseteq p_1
\]

Suppose \( y \in (a : x) \). Then \( xy \in a \subseteq q_1 \) but \( x \notin q_1 \). Since \( q_1 \) is primary this implies \( y^m \in q_1 \) which means \( y \in r(q_1) = p_1 \) which is what we needed to show. \( \square \)

Definition 4.11. A prime \( p_i \) as above is called a minimal associated prime if it does not contain any other associated prime. The others are called embedded primes.

Exercise 4.12. If \( a = r(a) \) then \( a \) has no embedded primes.

Proposition 4.13. \( \bigcup p_i \) is equal to the set of zero divisors modulo \( a \).

This is a corollary of the proof of the theorem above.

4.3. saturation. To get the next theorem we needed to review what we learned last time.

1. If \( S \) is a multiplicative set in \( A \), there is a 1-1 correspondence between the prime ideals in \( A \) which don’t meet \( S \): \( p \cap S = \emptyset \) and the prime ideals of \( S^{-1}A \) given by \( p \mapsto p^e = S^{-1}p \) and in the other direction, \( q^e = q \cap A \leftarrow q \subseteq S^{-1}A \).

2. If \( p \cap S \neq \emptyset \) then \( p^e = S^{-1}p = S^{-1}A \).

Definition 4.14. If \( S \subseteq A \) is a multiplicative set the saturation \( S(a) \) of an ideal \( a \) is the contraction of its extension:

\[
S(a) = a^e = S^{-1}a \cap A
\]
(Actually, this notation isn’t technically correct since $f : A \to S^{-1}A$ may not be injective. The intersection just means the inverse image in $A$.)

With this notation we can rephrase the bijective correspondence:

1. $S(p) = p$ if $p \cap S = \emptyset$.
2. $S(p) = A$ if $p \cap S \neq \emptyset$

**Lemma 4.15.** Suppose that $a = \bigcap q_i$ is a minimal primary decomposition and $S$ is a multiplicative set which is disjoint from the first $m$ primary ideals: $q_i \cap S = \emptyset$ for $i = 1, \ldots, m$ and $q_j \cap S \neq \emptyset$ for $j > m$. Then

$$S(a) = \bigcap_{i=1}^{m} q_i$$

**Proof.** First of all

$$S^{-1}a = S^{-1}\bigcap_{i=1}^{n} q_i = \bigcap_{i=1}^{n} S^{-1}(q_i)$$

because $S^{-1}$ is an exact functor (Prop 3.19 (i)). Contraction also commutes with intersection. So

$$S(a) = f^{-1}S^{-1}a = \bigcap_{i=1}^{n} f^{-1}S^{-1}(q_i) = \bigcap_{i=1}^{n} S(q_i) = \bigcap_{i=1}^{m} q_i$$

where at the last step we use the following easy facts.

1. $S(q_i) = q_i$ if $q_i \cap S = \emptyset$ (i.e., for $i \leq m$)
2. $S(q_i) = A$ if $q_i \cap S \neq \emptyset$ (i.e., for $i > m$).

□

**Theorem 4.16.** If $a$ has a primary decomposition $a = \bigcap q_i$ then the primary components $q_i$ corresponding to the minimal primes $p_i$ are uniquely determined by $a$.

**Proof.** The minimal primes are uniquely determined by the previous theorem. If $p_1$ is a minimal prime, let $S_1 = A - p_1$ be the complement of $p_1$. Then $S_1$ is disjoint from $q_1$ but $S_1$ meets $q_i$ for every $i > 1$ since otherwise $p_i \subseteq p_1$ contradicting the minimality of $p_1$. By the lemma we have:

$$S_1(a) = q_1$$

□

**Exercise 4.17.** The $n$th **symbolic power** $p^{(n)}$ of a prime ideal $p$ is defined to be the saturation $S(p^n)$ where $S = A - p$. Show that if $p^n$ has a primary decomposition then one of the components is $p^{(n)}$. 
5. Integral dependence and valuation

This section is about integral extensions and the integral closure of a ring.

5.1. Integral extensions.

Definition 5.1. Suppose that $A$ is a subring of $B$. We say that $B$ is an integral extension of $A$ if every element of $B$ is integral over $A$. Recall that $b \in B$ is integral over $A$ if $b$ is a root of a monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

with coefficients $a_i \in A$. (In other words, $f(b) = 0$.)

If $f(b) = 0$ then every power of $b$ can be written as an $A$-linear combination of the powers

$$1, b, b^2, \ldots, b^{n-1}$$

So, every element of $A[b]$ can be written as an $A$-linear combination of these $n$ elements.

Lemma 5.2. $A[b]$ is finitely generated as an $A$-module (if $b$ is integral over $A$).

The set of all elements of $B$ which are integral over $A$ is called the integral closure of $A$ in $B$ and we call it $C$. We will show that $C$ is a subring of $B$ containing $A$. We say that $A$ is integrally closed in $B$ if $C = A$.

Example 5.3. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

To prove this take any element of $\mathbb{Q}$ which is integral over $\mathbb{Z}$ and write it in reduced form: $x/s$ where $x, s$ are relatively prime. Then

$$\left(\frac{x}{s}\right)^n + a_1 \left(\frac{x}{s}\right)^{n-1} + \cdots + a_n = 0$$

$$x^n + a_1 x^{n-1} s + \cdots + a_n s^n = 0$$

This implies that $s$ divides $x^n$. So, $s = \pm 1$.

Exercise 5.4. Show that any UFD is integrally closed in its field of fractions.

Here are more things that follow just from the definition:

Proposition 5.5. Suppose that $B$ is an integral extension of $A$.

1. Let $a = A \cap b$ (so that $A/a \subseteq B/b$) then $B/b$ is an integral extension of $A/a$.
2. $S^{-1}B$ is an integral extension of $S^{-1}A$. 
Proposition 5.6. Suppose that $A$ is a subring of $B$ and $b \in B$. Then the following are equivalent.

1. $b$ is integral over $A$.
3. $A[b]$ is contained in a subring $M$ of $B$ which is a f.g $A$-module.
4. There is a f.g. $A$-module $M$ on which $A[b]$ acts faithfully.

$A[b]$ acts faithfully on $M$ means that the induced ring homomorphism $A[b] \rightarrow \text{End}(M)$ is injective. This is equivalent to saying that the annihilator of $M$ in $A[b]$ is zero.

Proof. (1) $\implies$ (2) by the lemma and (2) $\implies$ (3) is clear. Also (3) $\implies$ (4) since $A[b]$ acts faithfully on $M$ because $M$ contains $A[b]$: The composition $A[b] \rightarrow \text{End}(M) \rightarrow \text{End}(A[b])$ is injective. So, it suffices to prove that (4) $\implies$ (1). This follows from the determinant trick (Prop 2.3). Multiplication by $b$ induces an $A$-module homomorphism $\phi : M \rightarrow \text{a}M = M$ where $\text{a} = A$. Therefore there is a monic polynomial $f[x] \in A[x]$ so that $f(\varphi) = 0$ in $\text{End}(M)$. Since $M$ is a faithful $A[b]$ module, this implies that $f(b) = 0$ in $A[b]$. So, $b$ is integral over $A$. □

Corollary 5.7. If $A$ is a subring of $B$ and $B$ is a finite $A$-algebra (f.g. $A$-module) then $B$ is an integral extension of $A$.

Proof. Use (4). □

Corollary 5.8. If $b_1, \cdots, b_n \in B$ are integral over $A$ then $A[b_1, \cdots, b_n]$ is an integral extension of $A$.

Proof. Suppose that $f_i(x) \in A[x]$ are monic polynomials of degree $d_i$ so that $f_i(b_i) = 0$. Then any power of $b_i$ can be written as an $A$-linear combination of the powers

$$1, b_i, b_i^2, \cdots, b_i^{d_i-1}$$

So, every element of $A[b_1, \cdots, b_n]$ can be written as an $A$-linear combination of the monomials

$$b_1^{m_1}b_2^{m_2} \cdots b_n^{m_n}$$

where $m_i < d_i$. So, $A[b_1, \cdots, b_n]$ is f.g. $A$-module. So, all of its elements are integral over $A$. □

Corollary 5.9. If $B$ is an integral extension of $A$ and $C$ is an integral extension of $B$ then $C$ is an integral extension of $A$.

Corollary 5.10. If $A \subseteq C \subseteq B$ and $C$ is the integral closure of $A$ in $B$ then $C$ is integrally closed.
5.2. going up.

**Proposition 5.11.** Suppose that $A, B$ are integral domains and $B$ is an integral extension of $A$. Then $B$ is a field iff $A$ is a field.

**Proof.** Suppose $B$ is a field and $a \neq 0 \in A$. Then $B$ contains the inverse $a^{-1}$ of $a$ and, since $B$ is an integral extension, $a^{-1}$ is a root of a monic polynomial $f(x) \in A[x]$

$$a^{-n} + a_1a^{1-n} + a_2a^{2-n} + \cdots + a_n = 0$$

Multiplying by $a^{n-1}$ we get:

$$a^{-1} + a_1 + a_2a + a_3a^2 + \cdots + a_na^{n-1} = 0$$

Solving for $a^{-1}$ we see that $a^{-1} \in A$. So, $A$ is a field.

Conversely, suppose that $A$ is a field. Let $b \neq 0 \in B$. Then $b \in A[b]$ which is a finitely generated $A$ modules. In other words, $A[b] \cong A^n$ is a finite dimensional vector space over the field $A$. Multiplication by $b$ gives a linear mapping:

$$\mu_b : A[b] \cong A^n \rightarrow A^n = A[b]$$

Since $B$ is an integral domain, the kernel of $\mu_b$ is 0. This means that $\mu_b$ has rank $n$ and is therefore an isomorphism of vector spaces. So, it is onto. So, there is some $c \in B$ so that $\mu_b(c) = bc = 1$. So, $c = b^{-1} \in A[b] \subseteq B$ showing that $B$ is a field.

**Corollary 5.12.** Suppose that $B$ is an integral extension of $A$ and $q$ is a prime ideal in $B$. Then $q$ is maximal in $B$ iff $p = q^c = q \cap A$ is maximal in $A$.

**Theorem 5.13.** Any integral extension $f : A \hookrightarrow B$ induces an epimorphism

$$f^* : \text{Spec}(B) \twoheadrightarrow \text{Spec}(A)$$

**Proof.** Suppose $p \in \text{Spec}(A)$. Let $S = A - p$ then $S^{-1}A = A_p$ is a local ring and $B_p = S^{-1}B$ is an integral extension of $A_p$ by Proposition [5.5].

We have the following commuting diagrams of rings and induced maps on spectra:

$$\begin{array}{ccc}
A & \rightarrow & B \\
\downarrow & & \downarrow \\
A_p & \rightarrow & B_p \\
\end{array} \quad \begin{array}{ccc}
\text{Spec}(A) & \leftarrow & \text{Spec}(B) \\
\uparrow & & \uparrow \\
\text{Spec}(A_p) & \leftarrow & \text{Spec}(B_p) \\
\end{array}$$

Let $n$ be any maximal ideal in $B_p$. Then, by the corollary above, $m = n \cap A_p$ is a maximal ideal in $A_p$. Since $A_p$ has a unique maximal ideal $m = S^{-1}p$ which contracts to $p \in \text{Spec}(A)$. By commutativity of the diagram, $q = n \cap B \in \text{Spec}(B)$ maps to $p \in \text{Spec}(A)$.
Theorem 5.14 (Going up Theorem). Suppose \( p \subseteq p' \) are prime ideals in \( A \) and \( B \) is an integral extension of \( A \). Let \( q \) be a prime ideal in \( B \) which maps to \( p \). Then \( B \) contains a prime \( q' \supseteq q \) so that \( q' \) maps to \( p' \).

Proof. This is equivalent to saying that
\[ \text{Spec}(B/q) \rightarrow \text{Spec}(A/p) \]
is surjective. \( \square \)

Exercise 5.15. If \( A \subseteq B \) is an integral extension then show that
\[ \text{Spec}(B) \rightarrow \text{Spec}(A) \]
is a closed map (sends closed sets onto closed sets).

5.3. going down.

Definition 5.16. An integral domain is said to be integrally closed if it is integrally closed in its field of fractions.

Lemma 5.17. Suppose that \( A \subseteq C \subseteq B \) and \( C \) is the integral closure of \( A \) in \( B \). Then, for any multiplicative subset \( S \) of \( A \), \( S^{-1}C \) is the integral closure of \( S^{-1}A \) in \( S^{-1}B \).

Proposition 5.18. Suppose that \( A \) is an integral domain. Then the following are equivalent.

1. \( A \) is integrally closed.
2. \( A_p \) is integrally closed for every prime ideal \( p \).
3. \( A_m \) is integrally closed for every maximal ideal \( m \).

Note that \( A_p, A_m \) are all subrings of the field of fractions \( Q(A) \) of \( A \).

Proof. (1) \( \Rightarrow \) (2) by the lemma and (2) \( \Rightarrow \) (3) is clear.

To prove (3) \( \Rightarrow \) (1), let \( C \) be the integral closure of \( A \) in \( Q(A) \). We want to show that the inclusion map \( f : A \rightarrow C \) is an isomorphism. The lemma implies that \( C_m \) is the integral closure of \( A_m \) in \( Q(A) = Q(A_m) \). So, (3) implies that \( f_m : A_m \rightarrow C_m \) is the identity map for all maximal ideals \( m \). Since being an isomorphism is a local property this implies that \( f \) is an isomorphism. \( \square \)

Definition 5.19. If \( a \) is an ideal in \( B \) and \( b \in B \) we say that \( b \) is integral over \( a \) if it is a root of a monic polynomial
\[ f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n \]
with all \( a_i \in a \). In other words, \( f(x) \equiv x^n \) modulo \( a \). We say that \( a \) is integrally closed in \( B \) if it contains all elements of \( B \) which are integral over \( a \).
Lemma 5.20. Suppose \( a \) is an ideal in \( A \) and \( b \in B \) where \( B \) is an integral extension of \( A \). Then the following are equivalent.

1. \( b \) is integral over the ideal \( a \)
2. \( b^n \) is integral over \( a \) for some \( n \geq 1 \)
3. \( b^n \in aB \) for some \( n \geq 1 \).

In particular, if \( a \) is integrally closed in \( B \) then \( a = \sqrt{a} \) since (3) holds for any \( b \in \sqrt{a} \).

Proof. It is clear that (1) \( \iff \) (2) \( \Rightarrow \) (3). The last step (3) \( \Rightarrow \) (1) follows from the determinant trick (Proposition 2.3) which says that if \( \varphi \) is an endomorphism of an f.g. \( A \)-module \( M \) so that \( \varphi(M) \subseteq aM \) then \( \varphi \) satisfies a monic polynomial equation

\[
\varphi^m + a_1\varphi^{m-1} + \cdots + a_m = 0
\]

where \( a_i \in a \). (3) implies that

\[
b^n = \sum_{i=1}^{k} a_i'b_i
\]

for some \( a_i' \in a \) and \( b_i \in B \). Let \( M = A[b_1, \ldots, b_k] \) be the subring of \( B \) generated by \( A \) and the elements \( b_i \). Then \( M \) is a finitely generated \( A \)-module since the elements \( b_i \) are all integral over \( A \) and \( b^n \in M \). Let \( \varphi : M \rightarrow M \) be multiplication by \( b^n \). Then the above equation for \( b^n \) shows that \( \varphi(M) \subseteq aM \). So, \( \varphi \) satisfies a monic polynomial equation as above. If we apply this to \( 1 \in M \) we get

\[
b^nm + a_1b^{n(m-1)} + \cdots + a_m = 0
\]

showing that \( b^n \) and \( b \) are integral over \( a \). \( \square \)

Lemma 5.21. Let \( a \) be an ideal in \( A \) and \( A \subseteq B \). Let \( C \) be the integral closure of \( A \) in \( B \). Then the integral closure of \( a \) in \( B \) is equal to the radical in \( B \) of the extension \( a^c = Ca \) of \( a \) in \( C \). In particular, the integral closure of \( a \) in \( B \) is closed under addition and multiplication.

Proof. If \( b \) is integral over \( a \) then it is integral over \( A \) and thus lies in \( C \). But then the monic polynomial equation that it satisfies gives \( b^n \in aC \). This is the same as saying that \( b \in \sqrt{aC} \). \( \square \)

Proposition 5.22. Let \( A \subseteq B \) be integral domains, \( A \) integrally closed and let \( b \in B \) be integral over \( a \subseteq A \). Then \( b \) is algebraic over the field of fractions \( Q(A) \) of \( A \) and its minimal polynomial has coefficients in \( \sqrt{a} \) except for the leading coefficient of 1.
Proof. If $b$ is integral over $a$ then $b$ is integral over $A$ and therefore algebraic over $Q(A)$. The minimal polynomial $f(x)$ of $b$ is a product

$$f(x) = \prod (x - b_i)$$

where $b_i$ are Galois conjugates of $b$. The polynomial $f(x)$ divides the monic polynomial with coefficients in $a$ of which $b$ is a root. Therefore, all $b_i$ are also integral over $a$. The coefficients of $f(x)$ are sums of products of the $b_i$ and are therefore also integral over $a$. They also lie in $Q(A)$. Since $A$ is integrally closed, this implies that these coefficients lie in $r(a)$ by the lemma (and the radical of $a$ in $A$ is equal to the radical of $a$ in $Q(A)$).

□

Theorem 5.23 (Going down Theorem). Suppose that $A, B$ are integral domains, $A$ is integrally closed and $B$ is an integral extension of $A$. Suppose that $q_1$ is a prime ideal in $B$ and $p_1 = q_1^c = q_1 \cap A$ is the corresponding prime ideal in $A$. Then any prime ideal $p_2 \subseteq p_1$ in $A$ is the contraction of a prime ideal $q_2 \subseteq q_1$ in $B$.

Proof. Since $Spec B_{q_1}$ is the set of prime ideals in $B$ which are contained in $q_1$, this is equivalent to saying that $p_2$ is the contraction of some ideal in $B_{q_1}$. Using the bijection between contracted and extended ideals, this is equivalent to saying that:

$$p_2 = p_2^e = B_{q_1}p_2 \cap A.$$ 

Suppose this is not true. Then there is some $x \in B_{q_1}p_2 \cap A$ so that $x \notin p_2$ and we will get a contradiction proving the theorem.

Since $B_{q_1}p_2 = S^{-1}Bp_2$ where $S = B - q_1$ any $x \in B_{q_1}p_2$ has the form $x = y/s$ where $y \in Bp_2$ and $s = yx^{-1} \in S$. By (3) $\Rightarrow$ (1) in the lemma, this implies that $y$ is integral over $p_2$. By the proposition above, the minimal polynomial of $y$ over $Q(A)$ is monic with other coefficients in $p_2$:

$$y^n + a_1y^{n-1} + \cdots + a_n = 0$$

where $a_i \in p_2$. Multiplying by $x^{-n} \in Q(A)$ we see that the minimal polynomial of $s = y/x$ over $Q(A)$ is

$$s^n + (a_1x^{-1})s^{n-1} + \cdots + a_nx^{-n} = 0$$

Since $s \in B$, it is integral over $A$. So, the proposition says that all coefficients $a_ix^{-i}$ are in $A$. But $x \notin p_2$ and $a_i \in p_2$ imply $a_ix^{-i} \in p_2$. So,

$$s^n \in p_2B \subseteq p_1B \subseteq q_1$$

which is a contradiction. □
5.4. **valuation rings.** Suppose that $K$ is any field. Then a **valuation ring** of $K$ is any subring $B$ so that for any nonzero $x \in K$ either $x \in B$ or $x^{-1} \in B$. In other words, 

$$K = B \cup B^{-1}$$

where $B^{-1}$ denotes the set of all inverses of nonzero elements of $B$.

**Example 5.24.**

1. $K = \mathbb{Q}$ and $B = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid p \nmid b \right\}$ where $p$ is a prime number.
2. $K = k(x) = \mathbb{Q}(k[x])$ and $B = \left\{ \frac{f(x)}{g(x)} \mid \deg f \geq \deg g \text{ (or } f(x) = 0) \right\}$

**Exercise 5.25.**

1. $K = \mathbb{Q}(B)$.
2. Show that for any two ideals $a, b \subseteq B$, either $a \subseteq b$ or $b \subseteq a$.

**Proposition 5.26.**

1. $B$ is a local ring.
2. $B - m = B \cap B^{-1}$.
3. If $B'$ is a subring of $K$ containing $B$ then $B'$ is also a valuation ring and $m' \subseteq m$.
4. $B$ is integrally closed (in $K$). ($x \in K$ is integral over $B$ iff $x \in B[x^{-1}]$.)

One of the main purposes of valuation rings is to relate fields of different characteristics. Often we take $K$ to have characteristic 0 and the field $B/m$ to have characteristic $p$. For this purpose, we can start with a field $K$ and we look for subrings $A \subseteq K$ with homomorphisms $A \to \Omega$ where $\Omega$ is another field.

Let $\Sigma = \Sigma(K, \Omega)$ be the set of all pairs $(A, f)$ where $A$ is a subring of a field $K$ and $f : A \to \Omega$ is a homomorphism to another field which is algebraically closed. Then $\Sigma$ is partially ordered by $(A, f) \leq (A', f')$ is $A \subseteq A'$ and $f = f'|A$.

By Zorn’s lemma, $\Sigma$ contains a maximal element, say $(B, g)$. We will show that $B$ is a valuation ring for $K$.

**Lemma 5.27.** $B$ is a local ring with unique maximal ideal $m = \ker g$.

**Proof.** First note that $m = \ker g$ is a prime ideal since $B/m \hookrightarrow \Omega$. If $m$ is not maximal then $B \subsetneq B_m$ and it is easy to see that there is a unique extension of $g : B \to \Omega$ to $B_m$ contradicting the maximality of $(B, g)$. \qed
Exercise 5.28. 1) If we have a prime ideal in a subring of a field: \( p \subseteq A \subseteq K \) then \( A_p \) is a subring of \( K \) with unique maximal ideal \( m = pA_p \) and \( m \cap A = p \).

2) Show that \((B, m)\) is maximal in the poset of all pairs \((A, p)\) where \( p \) is a prime ideal in \( A \subseteq K \) and the partial ordering is \((A, p) \leq (A', p')\) if \( A \subseteq A' \) and \( p = A \cap p' \). [If \((B, m) \leq (B', m')\) show that \( B'/m' \) is an algebraic field extension of \( B/m \).]

Theorem 5.29. Any maximal \((B, g)\) in \( \Sigma \) is a valuation ring in \( K \).

Proof. We will prove the stronger statement that any \((B, m)\) which is maximal in the sense of the above exercise is a valuation ring in \( K \).

Suppose that \( B \) is not a valuation ring. Then there is some \( x \in K \) so that \( x, x^{-1} \notin B \). Let \( B' = B[x] \). Then the extended ideal \( m[x] \) is either contains 1 or it doesn’t. In the second case \( m[x] \) is contained in a maximal ideal \( m' \subseteq B' \) and \( m' \cap B = m \) contradicting the exercise above. Therefore, \( 1 \in m[x] \). So

\[
1 = a_0 + a_1 x + \cdots + a_n x^n
\]

for some \( a_i \in m \). Similarly, \( x^{-1} \notin B \) implies that

\[
1 = b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}
\]

for some \( b_i \in m \). By induction we may assume \( n, m \) are minimal and by symmetry we may assume that \( n \leq m \). Subtract \( a_0 \) from both sides of the first equation.

\[
1 - a_0 = a_1 x + \cdots + a_n x^n
\]

Then \( 1 - a_0 \) is a unit in \( B \) so we can divide to get

\[
1 = a'_1 x + \cdots + a'_n x^n
\]

Multiply by \( x^{-m} \) to get:

\[
x^{-m} = a'_1 x^{1-m} + \cdots + a'_n x^{n-m}
\]

Since \( m \geq n \) the exponents are \( \leq 0 \). Substitute into the second equation above and we get another expression for \( x^{-1} \) with a smaller \( m \). This contradicts the minimality of \( m \) proving the theorem.

Corollary 5.30. If \( A \) is a subring of \( K \), the integral closure \( \overline{A} \) of \( A \) in \( K \) is equal to the intersection of all valuation rings \( B \) which contain \( A \).

Proof. Since every \( B \) is integrally closed, \( \overline{A} \) is contained in every valuation ring \( B \supseteq A \). Conversely, suppose that \( x \in K \) is not integral over \( A \). Then we need to show that there is some valuation ring \( B \) which does not contain \( x \).
Since $x$ is not integral over $A$, $x \notin A' = A[x^{-1}]$. Since $x^{-1} \in A'$ is not a unit in $A'$, it is contained in some maximal ideal $m$. Then $(A, m)$ is an element of the poset in the exercise. By Zorn’s lemma, there is a maximal $(B, m') \geq (A, m)$. By the theorem, $B$ is a valuation ring which does not contain $x$ since $x^{-1} \notin m'$.

**Homework:** Do exercise 16 on page 69. We need this later in the book. The statement is:

**Theorem 5.31** (Noether’s normalization lemma). Let $k$ be a field and $A \neq 0$ a finitely generated $k$-algebra. Then there exist elements $y_1, \cdots, y_r \in A$ which are algebraically independent over $k$ so that $A$ is integral over $k[y_1, \cdots, y_r]$.

Solution of Exercise 5.28(2). If $(B, m)$ is not maximal in the poset then there is some $(A, p)$ which is larger. But, by part (1), $(A, p) \leq (A_p, m)$ where $m = pA_p$. Therefore, we may assume that $p$ is maximal. The next step is to show that if $(B, m) \leq (B', m')$ then $B'/m'$ is an algebraic extension of $B/m$. This is sufficient get a contradiction proving the theorem since $\Omega$ is algebraically closed and so the embedding $B/m \hookrightarrow \Omega$ extends to an embedding $B'/m' \hookrightarrow \Omega$ contradicting the assumed maximality of $(B, g)$.

To prove that $k' = B'/m'$ is algebraic over $k = B/m$, take any $x \in B'$, $x \notin m'$. Let $\pi$ be the image of $x$ in $k'$. Then $k \subseteq k[x] \subseteq k'$. Suppose that $x$ is not algebraic. Then $k[x]$ is a polynomial ring in one generator. So, the embedding $g : k \hookrightarrow \Omega$ extends to a homomorphism $\tilde{g} : k[x] \to \Omega$ (sending $x$ to an arbitrary element of $\Omega$, say 0). This gives a homomorphism $B[x] \to \Omega$ by composition:

$$g' : B[x] \to k[x] \to \Omega$$

The mapping $B[x] \to k[x]$ is the composition

$$B[x] \subseteq B' \to B'/m'$$

whose image is $k[x]$. Then $(B[x], g') > (B, g)$ contradicting the maximality of $(B, g)$ in $\Sigma$. 

6. Chain conditions

I will skip the details of this section and explain them as needed in the next two sections (on Noetherian and Artinian rings resp.).

**Definition 6.1.** A collection of subsets of a set $S$ satisfies the **ascending chain condition** (acc) if every ascending sequence

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$

attains its maximum $A_n = \bigcup A_k$ at a finite stage. (So, $A_n = A_{n+1} = \cdots$) Similarly, a collection of subsets satisfies the **descending chain condition** (dcc) if every descending sequence

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

attains its minimum: $A_n = \bigcap A_k$ at a finite stage.

**Definition 6.2.** A ring $A$ is called **Noetherian** if it has the acc for ideals. A module $M$ over any ring is called **Noetherian** if it has the acc for submodules. A ring $A$ is called **Artinian** if it satisfies the dcc for ideals. A module $M$ over any ring is called **Artinian** if it satisfies the dcc for submodules.

It is clear that $A$ is a Noetherian/Artinian ring iff it is Noetherian/Artinian as a module over itself.

**Proposition 6.3.** A module $M$ is Noetherian iff every submodule is finitely generated.

**Proposition 6.4.** Given a short exact sequence of $A$-modules

$$0 \to M' \to M \to M'' \to 0$$

(1) $M$ is Noetherian iff both $M', M''$ are Noetherian.

(2) $M$ is Artinian iff both $M', M''$ are Artinian.

**Definition 6.5.** A **composition series** for a module $M$ is a finite strictly decreasing sequence of submodules:

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n = 0$$

so that every quotient $M_i/M_{i+1}$ is simple (has no nonzero proper submodules). The **length** of the composition series is the number $n$ (the number of simple subquotient modules).

**Theorem 6.6.** Any two composition series for $M$ have the same length.

We define the length of $M$ to be the length of any composition series.

**Theorem 6.7.** A module $M$ has a composition series iff it satisfies both acc and dcc.
7. Noetherian rings

A ring is Noetherian if it satisfied the ascending chain condition for ideal. Equivalently, every ideal is finitely generated. Equivalently, any nonempty collection of ideals has a maximal element.

**Proposition 7.1.** Any factor ring \( A/\mathfrak{a} \) of a Noetherian ring is Noetherian.

**Proposition 7.2.** If \( A \) is Noetherian, so is \( S^{-1}A \) for any multiplicative set \( S \).

**Lemma 7.3.** Any finitely generated module over a Noetherian ring is Noetherian. Any finite extension of a Noetherian ring is Noetherian.

**Theorem 7.4** (Hilbert basis theorem). If \( A \) is Noetherian then so is the polynomial ring \( A[x] \) and the power series ring \( A[[x]] \).

**Proof.** Let \( B = A[x] \) or \( A[[x]] \). Then \( B \) has a maximal ideal \( \mathfrak{m} = (x) \) which has the following two properties in both cases:

1. \( \bigcap \mathfrak{m}^n = 0 \)
2. The quotient \( B/(\mathfrak{m}^n) \) is isomorphic to \( A^n \) as \( A \)-module and is thus Noetherian by the lemma.

Let \( \mathfrak{a} \) be any ideal in \( B \). Then we claim that \( \mathfrak{a} \cap \mathfrak{m}^n \) is finitely generated for \( n \) sufficiently large. Since the quotient

\[
\frac{\mathfrak{a}}{\mathfrak{a} \cap \mathfrak{m}^n} \subseteq B/\mathfrak{m}^n
\]

is also finitely generated this will imply that \( \mathfrak{a} \) is finitely generated.

Now, I restrict to the case \( B = A[[x]] \). The other case is in the book and follows the same pattern.

Let \( \mathfrak{b} \) be the ideal generated by all lowest degree coefficients of all elements in \( \mathfrak{a} \). Let \( b_1, \ldots, b_n \) be generators for \( \mathfrak{b} \) and let \( f_i(x) \in \mathfrak{a} \) be power series with lowest degree terms \( b_i x^{m_i} \). Multiplying these by a power of \( x \) we may assume that the \( m_i \) are all equal to a fixed \( m \). Then we claim that \( f_i(x) \) generate the ideal \( \mathfrak{a} \cap \mathfrak{m}^m \). To show this, take any element \( g(x) \in \mathfrak{a} \cap \mathfrak{m}^m \). Let \( cx^m \) be the lowest degree term in \( g(x) \). Then \( c \in \mathfrak{b} \). So \( c = \sum c_i b_i \) for some \( c_1, \ldots, c_n \in A \) so

\[
g(x) - \sum c_i f_i(x) \in \mathfrak{a} \cap \mathfrak{m}^{m+1}
\]

Similarly, there exist \( c_i' \in A \) so that

\[
g(x) - \sum c_i f_i(x) - \sum c_i' x f_i(x) \in \mathfrak{a} \cap \mathfrak{m}^{m+2}
\]

Proceeding in this way we get \( g(x) = \sum h_i(x) f_i(x) \) as claimed. \( \Box \)
7.0.1. **Primary decomposition in Noetherian rings.** An ideal \( a \) in a ring \( A \) is called **irreducible** if it is not the intersection of two strictly larger ideals.

**Lemma 7.5.** Suppose \( A \) is Noetherian. Then

(1) Every ideal is a finite intersection of irreducible ideals.

(2) Every irreducible ideal is primary.

**Proof.** (1) Suppose not and let \( a \) be a maximal counterexample.

(2) If \( q \) is irreducible, we need to show it is primary. By passing to \( A/q \) we may assume that \( q = 0 \). Suppose that \( xy = 0 \) and \( y \neq 0 \) then we need to show that \( x^n = 0 \) for some \( n \geq 1 \). Since \( A \) is Noetherian, the sequence of ideals \((0 : x) = \text{Ann}(x) \subseteq \text{Ann}(x^2) \cdots \) stops at some \( \text{Ann}(x^n) = \text{Ann}(x^{n+1}) \). Then I claim that \( (x^n) \cap (y) = 0 \)

To see this take any element \( ax^n = by \). Then

\[
ax^{n+1} = byx = 0 \Rightarrow a \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n) \Rightarrow ax^n = 0
\]

Since 0 is an irreducible ideal, either \( (x^n) = 0 \) or \( (y) = 0 \). But \( y \neq 0 \). So, \( x^n = 0 \) showing that 0 is a primary ideal.

**Theorem 7.6.** Every ideal in a Noetherian ring has a primary decomposition.

**Lemma 7.7.** In a Noetherian ring any ideal \( a \) contains some power of its radical: \( r(a)^n \subseteq a \).

**Proof.** Suppose that \( a_i \) are generators for \( r(a) \). Then \( a_i^{m_i} \subseteq a \) for some \( m_i \). Then \( r(a)^{1+\sum(m_i-1)} \) is generated by monomials \( \prod a_i^{n_i} \) where \( \sum n_i = 1 + \sum(m_i - 1) \). So, at least one of the numbers \( n_i \geq m_i \) making each monomial an element of \( a \).

**Theorem 7.8.** The associated primes of an ideal \( a \) in a Noetherian ring are the prime ideals of the form \( (a : x) \) for some \( x \in A \).

**Proof.** If \( (a : x) = r(a : x) \) is prime then we know from before that it is an associated prime. Conversely, suppose that \( a = \bigcap q_i \) where \( q_i \) is \( p_i \)-primary. Let \( a_i = \bigcap_{j \neq i} q_i \). Let \( y \in a_i, \ y \notin a \). Then \( a \subseteq b = (a : y) = \bigcap(q_i : y) = (q_i : y) \subseteq p \)

So, \( r(b) = p_i \). So \( p_i^m \subseteq b \) for some \( m \geq 1 \). Take \( m \) minimal. Then \( p_i^{m-1} \not\subseteq b \). So, \( yp_i^{m-1} \not\subseteq a \). So \( \exists x \in yp_i^{m-1} \subseteq a_i, \ x \notin a \). But then

\[
 p_i \subseteq (a : x) = (q_i : x) \subseteq p_i
\]

showing that \( p_i \) has the desired form.
8. Artin rings

This section gives a complete description of Noetherian rings of (Krull) dimension 0 using the fact that they are semilocal.

Definition 8.1. A is an Artin ring if it satisfies the DCC for ideals. (Every nonempty set of ideals contains a minimal element.):

\[ A \supset a_1 \supset a_2 \supset \cdots \supset a_n = a_{n+1} = \cdots \]

(We will show: Artinian \(\iff\) Noetherian with dim 0.)

Example 8.2. \(\mathbb{Z}/n\) or any finite ring is Artinian.

Every field \(K\) is Artinian.

\(K[X]/(X^n)\) is an Artin ring.

Any algebra over a field \(K\) (containing \(K\) in its center) which is a fin dim vector space over \(K\) is Artinian.

\(\mathbb{Z}\) is not an Artin ring

\(K[X]\) is not an Artin ring

\(\implies\) not Artinian

Also, \(\mathbb{Z}\) and \(K[X]\) have dimension 1.

8.1. Krull dimension 0.

Lemma 8.3. Artinian domain \(\Rightarrow\) field.

Proof. Suppose not. Then \(\exists x \neq 0\) s.t. \(x\) is not a unit. Then

\[ A \supset (x) \supset (x^2) \supset \cdots \]

\[ A \text{ Artinian} \implies (x^n) = (x^{n+1}) \]

\[ \implies x^{n+1} = ax^{n+1} \]

\[ A \text{ has no z.d.} \implies 1 = ax \Rightarrow x \text{ is a unit} \]

\[ \Box \]

Proposition 8.4 (A-M 8.1). A Artinian \(\Rightarrow\) every prime is maximal.

Proof. \(A/p\) Artinian domain \(\Rightarrow\) field \(\Rightarrow\) \(p\) is maximal.

\[ \Box \]

Corollary 8.5. A Artin ring \(\Rightarrow\) dim \(A = 0\) (Krull dimension).

This follows immediately from the definition:

Definition 8.6. The Krull dimension \(d = \dim A\) is defined to be the length of the longest chain of prime ideals:

\[ p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_d \]

Example 8.7. \(\dim \mathbb{Z} = 1\) since \((0) \subsetneq (p)\)

\(\dim K[X_1, \cdots, X_n] = n\) since

\[ 0 \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n) \]
8.2. semilocal.

Corollary 8.8 (A-M 8.2). A Artin ring \( \Rightarrow \) nilrad \( A = \) Jacobson rad \( A \).

Proof.

\[
\text{nilrad } A = \bigcap p = \bigcap m = \text{Jacobson rad } A
\]

\( \square \)

Proposition 8.9 (A-M 8.3). An Artin ring has only finitely many maximal ideals.

Proof. If there were infinitely many maximal (prime) ideals we would get a descending chain:

\[
m_1 \supseteq m_1 \cap m_2 \supseteq m_1 \cap m_2 \cap m_3 \supseteq \cdots
\]

These are proper inclusions since

\[
m_1 \cap \cdots \cap m_n = m_1 \cap \cdots \cap m_{n+1}
\]

\[
\Rightarrow m_1 \cap \cdots \cap m_n \subseteq m_{n+1}
\]

\[
\Rightarrow m_i \subseteq m_{n+1} \quad \text{contradiction}
\]

by prime avoidance (Prop 1.11 in A-M).

\( \square \)

Definition 8.10. A ring \( A \) is called semilocal if it has only finitely many maximal ideals.

Corollary 8.11. Artinian \( \Rightarrow \) semilocal.

Proposition 8.12 (A-M 8.4). A Artinian \( \Rightarrow \) the nilradical (= Jacobson radical) is nilpotent.

Proof. Let \( n \) be the nilradical of \( A \). Thus

\[
n := \{ x \in A | x^n = 0 \text{ for some } n \}
\]

Then we want to show that \( n^m = 0 \) for some \( m \). By the DCC we have

\[
n \supset n^2 \supset \cdots \supset n^k = n^{k+1} = \cdots
\]

Suppose that \( n^k \neq 0 \). Then \( a = n \) is a solution of

\[
an^k \neq 0
\]

Let \( a \) be a minimal solution. Since \( an^k \neq 0 \), \( \exists a \in a \) so that \( an^k \neq 0 \).

So, \( (a)n^k \neq 0 \). By minimality of \( a \) this implies \( a = (a) \).

\[
an^k = an^{k+1} \neq 0 \Rightarrow \exists b \in n \text{ s.t. } abn^k \neq 0. \text{ So } (ab)n^k \neq 0 \text{ and we have } n = (a) = (ab). \Rightarrow \exists c \in A \text{ s.t. } a = abc \Rightarrow a = a(bc)^n \in n^n = 0. \text{ This is a contradiction.}
\]

\( \square \)
8.3. characterization of Artin rings. Recall 7.14 (7.7): In a Noetherian ring, every ideal \( a \) contains a power of its radical \( r(a) \). Taking \( a = 0 \) and \( r(0) = \text{nilrad } A \) we get:

**Corollary 8.13** (A-M 7.15). A Noetherian \( \Rightarrow \) \text{nilrad } A is nilpotent.

**Lemma 8.14.** Suppose \( m \subset A \) is a maximal ideal (\( A/m \) field) and \( A \) is Artinian or Noetherian. Then \( m/m^2 \) is a fin dim vector space over \( A/m \).

*Proof.* \( A/m^2 \) is Noetherian or Artinian and its proper ideals are exactly the vector subspaces of \( m/m^2 \). \qed

**Lemma 8.15** (A-M 6.11). Suppose that \( 0 \subset A \) is a finite product of (not necessarily distinct) maximal ideals \( 0 = m_1m_2 \cdots m_n \). Then the following are equivalent:

1. \( A \) is Noetherian.
2. \( A \) is Artinian.
3. Each quotient \( m_1 \cdots m_i/m_1 \cdots m_{i+1} \) is finite dimensional as a vector space over the field \( A/m_{i+1} \).

The proof is by induction on \( n \) using the exact sequence

\[
0 \rightarrow m_1 \cdots m_{n-1} \rightarrow A \rightarrow A/m_1 \cdots m_{n-1} \rightarrow 0
\]

**Theorem 8.16** (A-M 8.5). A Artinian \( \iff \) A Noetherian and \( \dim A = 0 \).

*Proof.* Both sides imply \( \dim A = 0 \). So, assuming \( \dim A = 0 \), we need to show \( A \) Artinian iff \( A \) Noetherian. By the lemma, it suffices to show that \( 0 \) is a finite product of maximal ideals.

(\( \Rightarrow \)) \( A \) Artinian \( \Rightarrow \) \( n = \cap m_i \) nilpotent (\( n^k = 0 \)). So, \( \prod m_i \subset \cap m_i = 0 \). So, \( A \) is Noetherian.

(\( \Leftarrow \)) \( A \) Noetherian \( \Rightarrow \) \( 0 \) has primary decomposition. So \( A \) has only finitely many minimal primes. But \( \dim A = 0 \) implies all primes are maximal. So, \( A \) has only finitely many maximal ideals \( m_i \). By 7.15 (8.13) this implies \( n = \cap m_i \) is nilpotent. By 6.11 (8.15), \( A \) is Artinian. \( \square \)

**Proposition 8.17.** Suppose \( A \) is Noetherian local with max ideal \( m \). Then either

1. \( m^n = 0 \) for some \( n \) (\( \Rightarrow \) \( A \) is Artin local) or
2. \( m^n \neq m^{n+1} \neq \cdots \)

*Proof.* By Nakayama (\( ma = a \iff a = 0 \)),

\[
m^n = m^{n+1} \iff m^n = 0
\]

\( \square \)
Theorem 8.18 (A-M 8.7: Structure thm for Artin rings).

\[ A \text{ Artin } \iff A \cong \prod_{i=1}^{n} A_i \] \( A_i : \text{Artin local} \)

Proof. (\(\Rightarrow\)) Suppose \( n^k = 0, n = \bigcap_{i=1}^{n} m_i. \)

Claim: \( A \xrightarrow{\varphi} \prod_{i=1}^{n} A/m_i^k \) is an isomorphism.

Proof: (Using properties of coprime ideals from [1.3.3])

\[ m_i \text{ coprime } \Rightarrow m_i^k \text{ coprime } \Rightarrow \{ \varphi \text{ onto and } \prod m_i^k = \cap m_i^k = 0 (\varphi \text{ is 1-1}) \}

(\(\Leftarrow\)) This follows from

Claim: \( A, B \text{ Artin } \Rightarrow A \times B \text{ Artin.} \)

Proof of claim: \( A \times 0 \rightarrow A \times B \rightarrow 0 \times B \) is a short exact sequence of \( A \times B \) modules where the first and third terms satisfy the DCC for submodules since the submodules of \( A \times 0 \) are the ideals in \( A \) and the submodules of \( 0 \times B \) are the ideals of \( B \). So, the middle satisfies the DCC for submodules = ideals.

Proposition 8.19 (A-M 8.8). If \( A \) is Artin local then TFAE:

1. Every ideal is principal.
2. \( m \) is principal.
3. \( \dim_k m/m^2 \leq 1 \) \( (k = A/m). \)

Proof. (1) \(\Rightarrow\) (2) \(\Rightarrow\) (3) is obvious. So, suppose (3).

Case 1. \( \dim_k m/m^2 = 0 \)

\[ \Rightarrow m = m^2 \Rightarrow NAK m = 0 \Rightarrow A = A/m = k \text{ is a field} \]
and \( 0 = (0) \) is the only ideal.

Case 2. \( \dim_k m/m^2 = 1 \)

\[ \Rightarrow m = (x) \Rightarrow m^r = (x^r) \]
\( m = \text{rad} A \text{ is nilpotent } (m^n = 0) \)

Claim: These are all the ideals of \( A. \)

Proof: Let \( a \subset A \) be a nontrivial proper ideal.

\[ a \neq A \Rightarrow a \subset m \quad a \neq 0 \Rightarrow a \nsubseteq m^n = 0 \]

So, \( a \subset m^r, a \nsubseteq m^{r+1} \) for some \( r \)

\[ \Rightarrow m^{r+1} \nsubseteq a + m^{r+1} \subset m^r \Rightarrow a + m^{r+1} = m^r \Rightarrow NAK a = m^r \]
which shows (1). The book proof of the last line is:

\[ \exists y = ax^r \in a, y \nsubseteq m^{r+1} \Rightarrow a \nsubseteq m \Rightarrow a : \text{unit } \Rightarrow x^r \in a \Rightarrow a = (x^r) = m^r \]
8.4. examples, problems.

Example 8.20. \( A = k[x_1, x_2, \cdots] \) is \( \infty \) generated, \( a = (x_1, x_2^2, x_3^3, \cdots) \). Then \( B = A/a \) is local with unique maximal ideal \( m = (x_1, x_2, \cdots) \). Also \( m \) is the unique prime ideal. So, \( \dim B = 0 \). But \( m \) is not nilpotent. So, \( A \) is not Artinian and not Noetherian. In fact, \( m \) is not finitely generated.

Example 8.21. \( A = k[x^2, x^3]/(x^4) \subset k[x]/(x^4) \). Then \( A \) is Artin local, \( m = (x^2, x^3) \), \( m^2 = 0 \) and \( \dim m = \dim m/m^2 = 2 \).

Problem. Show that a local ring \( A \) with maximal ideal \( m \) is Artinian iff \( m \) is nilpotent and \( m/m^2 \) is a finite dimension vector space over \( A/m \).

Use the fact that there is an epimorphism from the \( n \)-fold tensor power of \( m/m^2 \) onto \( m^n/m^{n+1} \).

Problem #6, p.92 A Noetherian, \( q \) a \( p \)-primary ideal. Consider chains of primary ideals from \( q \) to \( p \). Show that all such chains are bounded and all maximal chains have the same length.

Step 1. We may assume \( q = 0 \).

Proof: For simplicity suppose the maximal length is 3:

\[ q \subset q_1 \subset q_2 \subset p \text{ in } A \]

\[ 0 \subset q_1/q \subset q_2/q \subset p/q \text{ in } A/q \]

\( p/q \) is prime in \( A/q \). \( q_i/q \) are \( p/q \)-primary and distinct. So, there is a 1-1 correspondence between \( p \)-primary ideals between \( q \) and \( p \) and \( p/q \)-primary ideals between 0 and \( p/q \). So, we may replace \( A \) by \( A/q \) and assume that \( q = 0 \).

Step 2. 0 is \( p \)-primary \( \Rightarrow \) \( A - p \) has no zero divisors.

Proof: If \( s \in A - p \) is a z.d. then \( st = 0 \) for some nonzero \( t \). But 0 is \( p \)-primary. So, either \( t = 0 \) or \( s^2 = 0 \). But both are impossible.

Step 3. \( S = A - p \) has no z.d. \( \Rightarrow a \leftrightarrow S^{-1}A = A_p \) and \( \forall p \)-primary \( q \):

1. \( S^{-1}q \) is \( S^{-1}p \)-primary
2. \( q^e = q \)

\( \Rightarrow \) There is a 1-1 correspondence between \( p \)-primary ideals in \( A \) and \( S^{-1}p \)-primary ideals in the local ring \( A_p \).

\[ A \quad A_p = S^{-1}A \]

\( p \)-primary \( q \) \( \leftrightarrow \) \( S^{-1}q = q^e S^{-1}p \)-primary

\( p \)-primary \( a^e \) \( \leftarrow \) \( a \) \( S^{-1}p \)-primary
Step 4. \( A_p \) is Artin local.

Proof: \( \dim A_p = 0 \). \( p \) is a minimal prime (It is the only prime associated to 0.)

Step 5 In an Artin local ring all ideals are \( \mathfrak{m} \)-primary.

\[
\begin{align*}
\dim \kappa \mathfrak{m}/\mathfrak{m}^2 &= d_1 \\
\dim \kappa \mathfrak{m}^i/\mathfrak{m}^{i+1} &= d_i \\
\dim \kappa \mathfrak{m}^n/\mathfrak{m}^{n+1} &= d_r \\
\mathfrak{m}^{r+1} &= 0 \quad d_{r+1} = 0 
\end{align*}
\]

Claim. All maximal chains of proper ideals have length \( d_1 + d_2 + \cdots + d_k \)

Proof: For each ideal \( a \) define

\[
a_i = \dim \kappa \frac{a \cap \mathfrak{m}^i + \mathfrak{m}^{i+1}}{\mathfrak{m}^{i+1}}
\]

(1) If \( a \subsetneq b \) then \( 0 \leq \sum a_i < \sum b_i \leq \sum d_i \)

(2) If \( \sum b_i - \sum a_i \geq 2 \) then \( \exists \ c \ s.t. \ a \subsetneq c \subsetneq b \) [Let \( i \) be minimal so that \( b_i > a_i \). Take \( b \in b \cap \mathfrak{m}^i, b \notin a \cap \mathfrak{m}^i + \mathfrak{m}^{i+1} \). Let \( c = a + (b) \). Then \( c_i = a_i + 1 \) and \( c_j = a_j \) for \( j \neq i \).]

Therefore, the numbers \( \sum a_i \) take all values from 0 to \( \sum d_i \) for any maximal chain of ideals.
8.5. **Nakayama’s Lemma.** Roger Lipsett wrote up the proof of the equivalence of various forms of Nakayama that we used in class.

**Theorem 8.22.** Let $A$ be a ring, $M$ be a finitely-generated $A$-module, $N$ a submodule of $M$, and $a$ an ideal of $A$ contained in its Jacobson radical. Then $M = aM + N \Rightarrow M = N$.

**Proof.** (This proof and the next are basically from A-M.) By the second isomorphism theorem for rings,

$$
\frac{aM + N}{N} = \frac{aM}{aM \cap N}
$$

and the obvious map

$$aM \to a \frac{M}{N} : am \mapsto a(m + N)$$

is surjective; the kernel is clearly $aM \cap N$. Thus

$$\frac{aM + N}{N} \cong \frac{M}{N}$$

So from $M = aM + N$ we get $M/N = a(M/N)$. Since $a$ is contained in the Jacobson radical of $M$, it is contained in the Jacobson radical of $M/N$, so by Nakayama, $M/N = 0$, i.e. $M = N$. □

Note that this theorem also implies Nakayama’s lemma - just set $N = 0$. So the two are equivalent.

**Theorem 8.23.** Let $A$ be a local ring with maximal ideal $m$ and residue field $k = A/m$, and $M$ a finitely generated $A$-module. Suppose $x_1, \ldots, x_n \in M$ are such that their images in $M/mM$ form a basis of $M/mM$ as a $k$-vector space. Then the $x_i$ generate $M$.

**Proof.** Let $N$ be the submodule of $M$ generated by the $x_i$; then $N \to M \to M/mmM$ is surjective, so that $N + mM = M$ so that $N = M$. □

So in the proof that $\dim_k m/m^2 = 1 \Rightarrow$ every ideal is principal, we have $\dim_k m/m^2 = 1 \Rightarrow m = (x)$ by Theorem 2, so that $m^r = (x^r)$. Also, $m$ is the radical of $A$ so is nilpotent. The claim was then that the $(x^r)$ are all the ideals of $A$. Let $a \subseteq A$ be a proper, nontrivial ideal, and choose $r$ with $a \subseteq m^r$, $a \not\subseteq m^{r+1}$. Then $m^{r+1} \not\subseteq a + m^{r+1} \subset m^r$; but $\dim_k m^r/m^{r+1} \leq 1$, so that in fact $a + m^{r+1} = m^r$. Now apply Theorem 1 with $N = a$, $M = m^r$, and $a = m$ to get $a = m^r$. 

9. Discrete valuation rings

9.1. discrete valuations. Recall the definition of a valuation ring. This is a subring $A$ of a field $K$ so that $K = A \cup A^{-1}$. In other words, for all $x \in K^* = K - 0$, either $x \in A$ or $x^{-1} \in A$. Many valuation rings (and all Noetherian valuation rings) are given by the following construction.

**Definition 9.1.** A discrete valuation on a field $K$ is a surjective function $v : K^* \rightarrow \mathbb{Z}$ so that

1. $v(xy) = v(x) + v(y)$. So, $v$ is a homomorphism ($\Rightarrow v(1) = 0$ and $v(x^{-1}) = -v(x)$.)
2. $v(x + y) \geq \min(v(x), v(y))$ assuming $x + y \neq 0$.

Extend $v$ to $0 \in K$ by letting $v(0) = +\infty$. Then both conditions above hold and

$$A = \{x \in K \mid v(x) \geq 0\}$$

is called the valuation ring of $v$.

An integral domain $A$ is called a discrete valuation ring if there is a discrete valuation $v$ on the field of quotients of $A$ so that $A$ is the valuation ring of $v$.

**Example 9.2.**

1. Let $K = \mathbb{Q}$ and for each prime $p$ let $v_p : \mathbb{Q}^* \rightarrow \mathbb{Z}$ be the function given by $v_p(p^ka/b) = k$ if $a, b$ are integers relatively prime to $p$. This is a discrete valuation with valuation ring equal to $\mathbb{Z}(p)$, the integers localized at the prime $(p)$.
2. Let $K = k(x)$, the field of rational functions $f(x)/g(x)$ in a variable $x$ with coefficients in a field $k$. Each nonzero polynomial $f(x)$ can be written uniquely as $f(x) = x^n f_0(x)$ where the constant term of $f_0(x)$ is nonzero. Let $v_x(f) = n$ and let

$$v_x(f/g) = v_x(f) - v_x(g)$$

This is a discrete valuation with valuation ring equal to $k[x]_{(x)}$, the polynomial ring $k[x]$ localized at the maximal ideal $(x)$.

**Proposition 9.3.**

1. $A$ is a local ring with unique maximal ideal $m = \{x \in K \mid v(x) \geq 1\}$
2. $m^n = \{x \in K \mid v(x) \geq n\}$
3. $m = (x)$ for any $x \in K$ with $v(x) = 1$.
4. $m^n = (x^n)$ for all $n \geq 1$
5. Every nonzero ideal in $A$ is equal to $m^n$ for some $n \geq 1$. 
Any $x$ as above is called a **uniformizer** of $A$. Note that each element of $A$ can be written uniquely in the form $ux^n$ where $u$ is a unit.

**Corollary 9.4.** $A$ is a Noetherian local domain with dimension 1.

Conversely, suppose that $A$ is a Noetherian local domain of dimension 1. Then $0$ and $m$ are the only prime ideals in $A$. So, all other ideals $a$ are $m$-primary. ($A/a$ has only one prime ideal. So, it is Artin local. So, the maximal ideal in $A/a$ is nilpotent which implies that $m^n \subseteq a$ for some $n$.)

**Proposition 9.5.** Suppose that $A$ is a Noetherian local domain with dimension one. Then the following are equivalent.

1. $m = (x)$ is principal.
2. $\dim_k m/m^2 = 1$ where $k = A/m$.
3. $m^n$ is principal for all $n \geq 1$
4. Every nonzero ideal in $A$ is equal to $m^n$ for some $n \geq 1$.
5. $A$ is a discrete valuation ring.
6. $A$ is integrally closed.

**Proof.** It is easy to see that the first 4 conditions are equivalent. Given these conditions, every element of $A$ can be written uniquely in the form $ux^n$ where $u$ is a unit. Then a discrete valuation on $A$ can be given by $v(ux^n) = n$ which is the largest number so that $m^n$ contains the element. This can be extended to a discrete valuation on the fraction field by $v(a/b) = v(a) - v(b)$. So, $A$ is a discrete valuation ring. So, $A$ is integrally closed by Prop. 5.26.

Finally, we show that (6) $\Rightarrow$ (1). Suppose not. Take $a \in m$, $a \notin m^2$. Then $(a)$ is $m$-primary. So there is an $n \geq 2$ so that $m^n \subseteq (a)$. Take $n$ minimal. Then there is some $b \in m^{n-1}$ so that $b \notin (a) = aA$.

Let $c = b/a \in K = Q(A)$. Then $b \notin aA \Rightarrow c \notin A$. So, $c$ is not integral over $A$ (A being integrally closed).

But $b \in m^{n-1} \Rightarrow bm \subseteq aA \Rightarrow cm \subseteq A$. Since this is an $A$-module, it is an ideal in $A$. But $cm$ is not contained in $m$. (Otherwise, $m$ would be a f.g. faithful $A[c]$-module contradicting the fact that $c$ is not integral over $A$. Therefore, $cm = A$. So, $bm = aA$. But this is a contradiction since $bm \subseteq m^2$ and $a \notin m^2$.)

**Exercise 9.6.** Show that a Noetherian domain is a valuation ring if and only if it is a discrete valuation ring.

**Exercise 9.7.** Given a discrete valuation ring $A$ with valuation $v : K^* \rightarrow \mathbb{Z}$ and uniformizer $x$, show that the $A$-submodules of $K$ are: $0$, $K$ and $x^nA$ for $n \in \mathbb{Z}$. (These are called fractional ideals.)
9.2. Dedekind domains.

**Definition 9.8.** A **Dedekind domain** is a Noetherian domain $A$ of dimension one satisfying any of the following equivalent conditions.

1. $A$ is integrally closed.
2. Every primary ideal in $A$ is a power of a prime ideal.
3. The localization $A_p$ of $A$ at any nonzero prime ideal is a discrete valuation ring.

For example, the ring of integers $\mathbb{Z}$ is a Dedekind domain since its primary ideals are $(p^k)$ for prime numbers $p$. The unique factorization of integers can be expressed as a unique factorization of ideals into products of powers of prime ideals:

$$n = \prod p_i^{k_i} \Rightarrow (n) = \prod (p_i)^{k_i}$$

To show that the conditions in the definition are equivalent, note that (1) $\iff$ (3) since “integrally closed” is a local condition. To show (2) $\iff$ (3) note that there is a bijection between $p$-primary ideals and the nonzero ideals in the local ring $A_p$.

**Theorem 9.9.** If $A$ is a Dedekind domain then every ideal $a$ can be expressed uniquely as a product of powers of prime ideals:

$$a = \prod p_i^{k_i}$$

**Proof.** Since $A$ is a domain with dimension 1, every nonzero prime ideal is maximal. Therefore, any two nonzero primes are coprime. So, any nonzero primary ideals with distinct radicals are coprime. So, in the primary decomposition of $a$ we can replace intersection with product and the terms are powers of prime ideals by the definition of a Dedekind domain.

**Theorem 9.10.** The ring of integers in any number field is a Dedekind domain.

A number field $K$ is a finite extension of the rational numbers. The ring of integers $A$ in $K$ is the integral closure of $\mathbb{Z}$ in $K$. In the “going up” theorem we showed that any prime ideal $p$ in $A$ is maximal if and only if $p \cap \mathbb{Z}$ is maximal in $\mathbb{Z}$. Also, if $p \subsetneq p'$ in $A$ then $p \cap \mathbb{Z} \subsetneq p' \cap \mathbb{Z}$. 

9.3. fractional ideals.

**Definition 9.11.** If $A$ is an integral domain with fraction field $K$ then by a fractional ideal of $A$ we mean an $A$-submodule $M \subseteq K$ so that $xM \subseteq A$ for some $x \neq 0 \in K$.

Here are some trivial observations.

1. Every ideal is a fractional ideal.
2. Any finitely generated $A$-submodule of $K$ is a fractional ideal.
3. $xM \cong M$ as an $A$-module.
4. If $A$ is a PID then every fractional ideal is also principal (generated by one element).
5. If $A$ is Noetherian, every fractional ideal is finitely generated.
6. $M$ is a fractional ideal if and only if $(A : M) \neq 0$

**Definition 9.12.** An $A$-submodule $M \subseteq K$ is an invertible ideal if $M(A : M) = A$

**Proposition 9.13.** $M$ is an invertible ideal iff there exist $x_1, \cdots, x_n \in M$ and $y_1, \cdots, y_n \in (A: M)$ so that

$$1 = \sum x_i y_i$$

**Corollary 9.14.** Every invertible ideal is a fractional ideal which is finitely generated. In fact it is generated by the elements $x_i$ in the above proposition.

**Proof.** Any $x \in M$ can be written as:

$$x = \sum (xy_i)x_i$$

where $xy_i \in A$ since $y_i M \subseteq A$.

**Corollary 9.15.** Suppose that $A$ is a local domain with unique maximal ideal $m$. Then $m$ is invertible if and only if it is principal.

**Proof.** If $m = (x)$ then $1 = xx^{-1}$ with $x^{-1} \in (A : m)$. So, $m$ is invertible.

Conversely, suppose the $m$ is invertible. Then

$$1 = \sum x_i y_i$$

where $y_i \in (A : m)$. The elements $x_i y_i$ cannot all be in $m$. So, at least one term, say $u = x_j y_j \in A - m$ is a unit. Then $1 = u^{-1} x_j y_j$ which implies that $m = (u^{-1} x_j) = (x_j)$ by the previous corollary. □

The property of being invertible is a local property of $M$. 

Proposition 9.16. Suppose that $M \subseteq K$ is an $A$-module. Then the following are equivalent.

1. $M$ is invertible.
2. $M$ is f.g. and $M_p$ is an invertible $A_p$ ideal for all prime ideals $p$ in $A$.
3. $M$ is f.g. and $M_m$ is an invertible $A_m$ ideal for all maximal ideals $m$ in $A$.

Note that all three conditions imply that $M$ is a fractional ideal.

Proof. Certainly (2) $\Rightarrow$ (3). To show (1) $\Rightarrow$ (2) we use the equation $1 = \sum x_i y_i$. We just need to recall that $(A : M)_p = (A_p : M_p)$ which holds since $M$ is finitely generated.

(3) $\Rightarrow$ (1). Let $M(A : M) = \mathfrak{a} \subseteq A$. If this is a proper ideal in $A$ then it is contained in a maximal ideal $\mathfrak{m}$ and we get $M_m(A_m : M_m) = \mathfrak{a}_m \subseteq \mathfrak{m}_m \subsetneq A_m$ which contradicts (3). Therefore $\mathfrak{a} = A$ and $M$ is invertible. $\square$

Proposition 9.17. Suppose that $A$ is a local domain. Then $A$ is a DVR iff every nonzero fractional ideal is invertible.

Proof. $\Rightarrow$: We did this already.

$\Leftarrow$: if every nonzero ideal is invertible then in particular the maximal ideal $\mathfrak{m}$ is invertible and thus principal. So, $A$ is a DVR. $\square$

Theorem 9.18. Suppose that $A$ is an integral domain. Then $A$ is Dedekind iff every fractional ideal is invertible.

Proof. Both conditions are local and imply that $A$ is Noetherian. $\square$

Corollary 9.19. The nonzero fractional ideals of a Dedekind domain form a group.

This group is called the group of ideals of $A$. It is an abelian group which the book calls $I$. The principal ideals form a subgroup $P$. The quotient $H$ is called the ideal class group of $A$. Since every principal ideal is generated by an element of $K^*$ we get a homomorphism $K^* \to P$ whose kernel is the group of units $U$ of $A$. This gives an exact sequence $1 \to U \to K^* \to I \to H \to 1$.

If $A$ is the ring of integers in a number field $K$ then it is well-known that $H$ is a finite group. The order of $H$ is called the class number of $K$. $U$ is a finitely generated group whose rank is given by the Dirichlet unit theorem which can be proved using Reidemeister torsion.
10. Completion

The real numbers are the completion of the rational numbers with respect to the usual absolute value norm. This means that any Cauchy sequence of rational numbers converges to a real number. These are sequences \((a_n)\) so that

\[ a_n - a_m \to 0 \]
as \(\min(n, m) \to \infty\). More precisely: Given any open neighborhood \(U\) of 0 in \(\mathbb{R}\), there is an integer \(N\) so that

\[ a_n - a_m \in U \]
for all \(n, m \geq N\).

In commutative algebra we are interested in completion with respect to valuations and ideals. Two main examples are

1. \(K[[x]]\) the ring of formal power series in \(x\)
   \[ \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots \]
   with coefficients \(a_i \in K\)

2. \(\mathbb{Z}_p\) the ring of \(p\)-adic integers.
   \[ \sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots \]
   with \(a_i \in \{0, 1, 2, \cdots, p - 1\}\)

The first example is the completion of \(K[x]\) since each element of \(K[[x]]\) is a limit of a sequence of elements of \(K[x]\). Similarly \(p\)-adic numbers are limits of integers. So \(\mathbb{Z}_p\) is a completion of \(\mathbb{Z}\).

Both of these are examples of \(a\)-adic completions.

10.1. \(a\)-adic topology.

**Definition 10.1.** A topological additive group is a group \(G\) with a topology so that *addition* and *negation* are continuous mappings

\[ (a, b) \mapsto a + b: \quad G \times G \to G \]
\[ a \mapsto -a: \quad G \to G \]

This is equivalent to the condition that *subtraction*

\[ (a, b) \mapsto a - b: \quad G \times G \to G \]
is continuous.

A subset \(V\) of \(G\) is open if and only, for all \(a \in U\) there is an open neighborhood \(U\) of 0 so that \(a + U \subseteq V\). Therefore, the topology on
G is uniquely determined by the open neighborhoods of 0. In fact we only to specify the basic open neighborhoods of 0.

Recall that a **basis** for a topology on a set X consists of a collections of subsets called **basic open sets** which have the property that

1. Every point \( x \in X \) lies in at least one basic open set. These are called the **basic open neighborhoods** of \( x \). [The basic open sets cover \( X \).]
2. For any two basic open neighborhoods \( U, V \) of \( x \) there is a third basic open neighborhood \( W \) so that \( x \in W \subseteq U \cap V \). [Equivalently, \( U \cap V \) is a union of basic open sets.]

We will take the basic open neighborhoods of 0 in \( G \) to be given by a descending sequence of subgroups

\[
H_1 \supseteq H_2 \supseteq H_3 \supseteq \cdots
\]

Then the basic neighborhoods of any \( g \in G \) are given by \( g + H_n \). Every open subgroup \( H_n \) is also a closed set in \( G \). Why is that? Also, \( G \) is Hausdorff if and only if

\[
\bigcap_n H_n = 0
\]

(*Hausdorff* means distinct elements of \( G \) lie in disjoint open sets.)

**Definition 10.2.** If \( a \) is an ideal in a ring \( A \) then the **\( a \)-adic topology** on \( A \) is the topology given by the ideals \( a^n \). Thus the basic open neighborhoods of \( x \in A \) are \( x + a^n \).

For any ideal \( a \), the **\( a \)-adic topology** makes \( A \) into a topological ring. We usually assume that

\[
\bigcap a^n = 0
\]

so that \( A \) is a Hausdorff topological ring.

There are two ways to define \( \hat{A} \), the **\( a \)-adic completion of \( A \)**. One is to let \( \hat{A} \) be the ring of all equivalence classes of Cauchy sequences of elements of \( A \). The other more convenient way is to take an inverse limit:

\[
\hat{A} := \lim_{\leftarrow} A/a^n
\]

10.1.1. **inverse limit.** We consider only **linear** inverse systems. These are sequences of groups and group homomorphisms

\[
\cdots \xrightarrow{\theta_{n+1}} G_n \xrightarrow{\theta_n} G_{n-1} \xrightarrow{\theta_{n-1}} \cdots \rightarrow G_2 \xrightarrow{\theta_2} G_1
\]

For example, a descending sequence of subgroups \( H_n \) of \( G \) gives such a sequence with \( G_n = G/H_n \). This linear system is called **surjective** if every homomorphism is surjective.
Definition 10.3. The (inverse) limit \( \lim G_n \) of a linear system of groups \( G_n \) is the subgroup of the direct product \( \prod G_n \) consisting of sequences \((g_1, g_2, \cdots)\) with \( g_n \in G_n \) so that \( \theta_n(g_n) = g_{n-1} \) for all \( n \geq 2 \).

Let \( p_n : \lim G_n \to G_n \) be the projection to the \( n \)-th coordinate. Then \( \theta_n \circ p_n = p_{n-1} \) and \( \lim G_n \) is clearly universal with this property:

Proposition 10.4 (universal property of inverse limit). The inverse limit satisfies the following universal property. Given any group \( H \) and homomorphisms \( f_n : H \to G_n \) so that \( \theta_n \circ f_n = f_{n-1} \), there is a unique homomorphism \( f_\infty : H \to \lim G_n \) so that \( p_n \circ f_\infty = f_n \) for all \( n \).

Proposition 10.5 (left exactness of inverse limit). Suppose that \((G_n, \theta_n)\) is a linear system of additive groups and \( H_n \) is a subgroup of \( G_n \) for each \( n \) so that \( \theta_n(H_n) \subseteq H_{n-1} \). Then \((G_n/H_n)\) is also a linear system of groups and we get the following exact sequence.

\[ 0 \to \lim H_n \to \lim G_n \to \lim G_n/H_n \]

Proof. Inverse limit is left exact since it is a right adjoint functor. Given any group \( H \), let \( C(H) \) be the constant system:

\[ H \to H \to H \to \cdots \to H \]

where all maps are the identity. Then the universal property of inverse limit can be rephrased as:

\[ \text{Hom}_D(C(H), (G_n)) \cong \text{Hom}(H, \lim G_n) \]

where \( D \) is the category of linear diagrams \((G_n)\) and compatible families of maps \( H_n \to G_n \).

However, in our special case: \( \mathfrak{a} \)-adic completion

\[ \widehat{M} = \lim M/\mathfrak{a}^n M \]

is an exact functor because of two theorems. The first is the vanishing of \( \lim^1 \) for surjective systems. The second is the Artin-Rees Lemma.

The theorem is the following.

Theorem 10.6. Completion at any ideal is an exact functor under certain finiteness conditions. In other words, an exact sequence \( 0 \to M' \to M \to M'' \to 0 \) induces an exact sequence

\[ 0 \to \widehat{M}' \to \widehat{M} \to \widehat{M}'' \to 0 \]

if certain conditions are satisfied.
Definition 10.7. Given a linear system $(A_n, \theta_n)$, let $A = \prod A_n$ and let $d^A : A \to A$ be the homomorphism given by

$$d^A(a_n) = (a_n - \theta_{n+1} (a_{n+1}))$$

So, $\lim A_n = \ker d^A$. Define $\lim^1 A_n$ to be the cokernel of $d^A$.

Lemma 10.8. If $(A_n)$ is a surjective system then $\lim^1 A_n = 0$.

Theorem 10.9. Given a short exact sequence of linear systems $0 \to (A_n) \to (B_n) \to (C_n) \to 0$, we get a 6-term exact sequence

$$0 \to \lim A_n \to \lim B_n \to \lim C_n \to \lim^1 A_n \to \lim^1 B_n \to \lim^1 C_n \to 0$$

In particular, if $(A_n)$ is a surjective system, we get a short exact sequence

$$0 \to \lim A_n \to \lim B_n \to \lim C_n \to 0$$

Proof. This follows from the snake lemma applied to the following diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
& & d^A & & d^B & & d^C & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}
$$

□

10.1.2. examples. Return to the two main examples $K[[x]]$ and $\mathbb{Z}_p$ to show these are $\mathfrak{a}$-adic completions.

Use this to find an example of an inverse system with nontrivial $\lim^1$:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{n+1}\mathbb{Z} & \longrightarrow & 0 \\
& & p & & = & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & 0
\end{array}
$$

This gives the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}_p \to \lim^1 (\mathbb{Z} \to \mathbb{Z}_p \to) \to 0$$

where $\lim^1 \mathbb{Z}$ is $\lim^1$ of the sequence of groups:

$$\cdots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to \cdots$$
10.2. **Artin-Rees.** Given an $A$-module $M$ and an ideal $\mathfrak{a}$ in $A$, recall that the $\mathfrak{a}$-adic completion of $M$ is defined to be the completion of $M$ with respect to the submodules $\mathfrak{a}^n M$:

$$\widehat{M} := \varprojlim M/\mathfrak{a}^n M$$

The two main theorems about completion assume that $A$ is Noetherian.

**Theorem 10.10.** If $A$ is Noetherian, completion at any ideal is an exact functor on finitely generated $A$-modules. In other words, an exact sequence $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ induces an exact sequence

$$0 \rightarrow \widehat{M}' \rightarrow \widehat{M} \rightarrow \widehat{M}'' \rightarrow 0$$

if $M', M, M''$ are finitely generated $A$-modules.

**Theorem 10.11.** If $A$ is Noetherian and $M$ is a finitely generated $A$-module then $\widehat{M} = \widehat{A} \otimes_A M$.

**Corollary 10.12.** If $A$ is Noetherian then $\widehat{A}$ is a flat extension of $A$.

It might seem that we have already shown the first theorem since we know that completion with respect to descending sequences of submodules is exact since the $\varprojlim$ terms are all zero. The only thing we need to show is that the induced sequences of submodules is eventually exact. This is the Artin-Rees Lemma.

10.2.1. **graded rings and modules.** Given any system of ideals in a ring or (more generally) submodules $M_n \subseteq M$, we can form two graded rings and modules.

**Definition 10.13.** A **graded ring** is a ring $A$ expressed as a direct sum $A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$ so that

$$A_n A_m \subseteq A_{n+m}$$

In particular, $A_0$ is a ring and each $A_n$ is a module over $A_0$. A **graded module** over a graded ring is a module $M$ together with a direct sum decomposition $M = M_0 \oplus M_1 \oplus M_2 \cdots$ so that

$$A_n M_m \subseteq M_{n+m}$$

One example is given by the following definition.

**Definition 10.14.** Given by an $A$-module $M$, a descending sequence of submodules:

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$
is called an $\mathfrak{a}$-filtration of $M$ if

$$\mathfrak{a}^n M_m \subseteq M_{n+m}$$

for all $n \geq 1, m \geq 0$. Clearly, this condition holds for all $n \geq 1$ iff it holds for $n = 1$. We say that the filtration is stable if equality holds in this condition for all sufficiently large $m$ and all $n \geq 1$.

**Definition 10.15.** Given an ideal $\mathfrak{a} \subseteq A$ and an $\mathfrak{a}$-filtration of an $A$-module $M$, let $A^*, M^*$ be given by

$$A^* := A \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots$$

$$M^* := M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$

The associated graded ring $\text{Gr}(A)$ and associated graded module $\text{Gr}(M)$ are defined by

$$\text{Gr}(A) = A/\mathfrak{a} \oplus A/\mathfrak{a}^2 \oplus A^3/\mathfrak{a}^3 \oplus \cdots$$

$$\text{Gr}(M) = M_0/M_1 \oplus M_1/M_2 \oplus \cdots$$

**Exercise 10.16.** Take $A = \mathbb{Z}$ and $\mathfrak{a} = (p)$. Show that $\mathbb{Z}^* \cong \mathbb{Z}[x]$ and $\text{Gr}(\mathbb{Z}) \cong \mathbb{Z}/(p)[x]$ as rings.

Show that $M^*$ is generated by $M_0$ iff $M_n = \mathfrak{a}^n M_0$ for all $n$.

**Lemma 10.17.** If $A$ is Noetherian then so is $A^* = A \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots$.

**Proof.** If $x_1, \cdots, x_n$ are generators for the ideal $\mathfrak{a}$ then $A^*$ is a quotient of the ring $A[x_1, \cdots, x_n]$ which is Noetherian by the Hilbert basis theorem and any quotient of a Noetherian ring is Noetherian. $\square$

**Lemma 10.18.** Suppose that $A$ is Noetherian, $M$ is finitely generated and $(M_n)$ is an $\mathfrak{a}$-filtration of $M$. Then $(M_n)$ is stable iff $M^*$ is a finitely generated $A^*$-module.

**Proof.** ($\Rightarrow$) Stability after stage $n$ implies that $M^*$ is generated by $M_0 \oplus M_1 \oplus \cdots \oplus M_n$ and each $M_n$ is f.g being a submodule of the f.g. $A$-module $M$.

($\Leftarrow$) Conversely, if $M^*$ is finitely generated with generators in, say, $M_0 \oplus M_1 \oplus \cdots \oplus M_n$ then

$$M_m = \mathfrak{a}^m M_0 + \mathfrak{a}^{m-1} M_1 + \cdots + \mathfrak{a}^{m-n} M_n = \mathfrak{a}^{m-n} M_n = \mathfrak{a} M_{m-1}$$

for all $m > n$ and $(M_n)$ is stable. $\square$

**Lemma 10.19** (Artin-Rees). If $A$ is Noetherian and $M$ is finitely generated, then for any submodule $N \subseteq M$, the filtration $(N \cap \mathfrak{a}^n M)$ of $N$ is stable.

**Proof.** Let $N^* = \bigoplus N \cap \mathfrak{a}^n M$. Then $(\mathfrak{a}^n M)$ stable $\Rightarrow M^*$ f.g. $\Rightarrow N^*$ f.g. (since $A^*$ is Noetherian) $\Rightarrow (N \cap \mathfrak{a}^n M)$ is stable. $\square$
Proof of Theorem 10.10. We can write our exact sequence as
\[ 0 \to N \to M \to M/N \to 0 \]
We have an \( a \)-filtration given by:
\[ 0 \to N \cap a^n M \to a^n M \to N + a^n M/N = a^n(M/N) \to 0 \]
By Artin-Rees the filtration of \( N \) is stable and therefore gives the same completion for \( N \) as does \( (a^n N) \). So, by exactness of inverse limit on surjective systems, we get
\[ 0 \to \hat{N} \to \hat{M} \to \hat{M}/\hat{N} \to 0 \]

10.2.2. equivalent filtrations. There is still one step missing in the proof.

Lemma 10.20. Any two stable \( a \)-filtrations of an \( A \)-module \( M \) give the same topology on \( M \) and therefore give isomorphic completions \( \hat{M} \).

Proof. It is easy to see that two systems of basic open neighborhoods \( U_\alpha, V_\beta \) of 0 in \( M \) give the same topology if and only if \( (\forall \alpha)(\exists \beta)V_\beta \subseteq U_\alpha \) and \( (\forall \beta)(\exists \alpha)U_\alpha \subseteq V_\beta \). If \( (M_n) \) is stable then \( a^n M_m = M_{n+m} \) for all \( m \geq m_0 \). So
\[ M_{n+m} = a^n M_m \subseteq a^n M \]
and by definition of an \( a \)-filtration we have
\[ a^n M \subseteq M_n \]

This implies that the sequence of submodules \( M_n \) gives the \( a \)-adic topology on \( M \). If we use the Cauchy sequence definition of completion we see that the two completions of \( M \) are the same. The reason is that the set of Cauchy sequences is determined by the topology of \( M \).

It remains to show that the two different descriptions of the completion of \( M \) are equivalent.

(1) \( \hat{M} \) is the module of equivalence classes of Cauchy sequences of elements of \( M \).

(2) \( \hat{M} \) is the inverse limit of \( M/a^n M \).

This is easy: when we take a family of compatible elements of \( M/a^n M \) and lift them to \( M \) we get a Cauchy sequence and conversely. \( \square \)

We still need to show Theorem 10.11 \( \hat{M} = \hat{A} \otimes_A M \).
10.2.3. flatness of $\hat{A}$. Since tensor product is right exact, we have the following diagram with exact rows.

$$
\begin{array}{c}
\begin{array}{c}
a^n \otimes_A M \\ 0
\end{array} \\
\begin{array}{c}
A \otimes_A M \\
M
\end{array} \\
\begin{array}{c}
A/a^n \otimes_A M \\
M/a^n M
\end{array} \\
\begin{array}{c}
0 \\
M/a^n M
\end{array}
\end{array}
\end{array}
$$

The map $\alpha$ is onto, the map $\beta$ is an isomorphism and this implies that $\gamma$ is also an isomorphism. The sequence of compatible isomorphisms $A/a^n \otimes_A M \to M/a^n M$ induces a sequence of adjoint maps:

$$
M \to \text{Hom}(A/a^n, M/a^n M)
$$

which induces a map

$$
M \to \text{Hom}(\hat{A}, \hat{M})
$$

whose adjoint is a natural map:

$$
\hat{A} \otimes_A M \to \hat{M}
$$

**Proposition 10.21.** If $M$ is a finitely generated $A$-module then this adjoint map is an epimorphism. If $A$ is also Noetherian then this map is also an isomorphism.

**Proof.** Let $F \to M$ be an epimorphism from a f.g. free module $F$ onto $M$ with kernel $N$. Then we have the following commuting diagram where the top row is exact.

$$
\begin{array}{c}
\begin{array}{c}
\hat{A} \otimes_A N \\
0
\end{array} \\
\begin{array}{c}
\hat{A} \otimes_A F \\
\hat{F}
\end{array} \\
\begin{array}{c}
\hat{A} \otimes_A M \\
\hat{M}
\end{array} \\
\begin{array}{c}
0 \\
0
\end{array}
\end{array}
\end{array}
$$

Here $\beta$ is an isomorphism since completion commutes with finite direct sum. This forces $\gamma$ to be an epimorphism.

If $A$ is Noetherian then the lower sequence is also exact and $\alpha$ is an epimorphism forcing $\gamma$ to be an isomorphism. \qed

Since $a$-adic completion is an exact functor on f.g. modules over a Noetherian ring, we get the following corollary.

**Corollary 10.22.** If $A$ is Noetherian then $\hat{A}$ is a flat $A$-module.

We say that $\hat{A}$ is a flat extension of $A$. 
10.3. properties of $\hat{A}$. The main theorem of the rest of this section is the following.

**Theorem 10.23.** A is Noetherian then $\hat{A}$ is Noetherian.

The proof is very convoluted and proves many important properties of completions along the way.

10.3.1. completeness of $\hat{A}$. The first property that we need is the completeness of $\hat{A}$ which uses the theorem from last time: $\hat{M} = \hat{A} \otimes_A M$ assuming that $A$ is Noetherian and $M$ is finitely generated. The case we need is $M = a$. Then

$$\hat{a} = \hat{A} \otimes_A a$$

The first property that we want to prove is that $\hat{A}$ is complete in the $\hat{a}$-adic topology.

**Proposition 10.24.** Suppose that $A$ is Noetherian and $a \neq (1)$ then

1. $\hat{a} \subseteq Jrad(\hat{A})$
2. $\hat{a}^n = \hat{a}^n$
3. $\hat{A}/\hat{a}^n \cong A/a^n$ for all $n \geq 1$
4. $\hat{a}^n/\hat{a}^{n+1} \cong a^n/a^{n+1}$ for all $n \geq 0$
5. $Gr(A) \cong Gr(\hat{A})$
6. $\hat{A}$ is complete in the $\hat{a}$-adic topology. ($\hat{A} = \hat{A}$)

**Proof.** Clearly (3) $\Rightarrow$ (4) $\Rightarrow$ (5) and (3) $\Rightarrow$ (6) since (3) tells us that the inverse system defining $\hat{A}$ is the same as the one defining $\hat{A}$.

To prove (3) I first proved a more general statement:

(3') $M/M_n \cong \hat{M}/\hat{M}_n$

Pf: Consider the following short exact sequence.

$$0 \rightarrow M_n/M_m \rightarrow M/M_m \rightarrow M/M_n \rightarrow 0$$

where $n$ is fixed and $m$ is going to $\infty$. This is a short exact sequence of surjective inverse systems where the last system is constant (does not change with $m$). So, it gives a short exact sequence of inverse limits:

$$0 \rightarrow \hat{M}_n \rightarrow \hat{M} \rightarrow M/M_m \rightarrow 0$$

For the case at hand this shows:

$$\hat{A}/\hat{a}^n \cong A/a^n$$

which becomes the same as (3) if we know that $\hat{a}^n = \hat{a}^n$. Therefore, (2) $\Rightarrow$ (3).
Statement (2) is the place where we need $A$ to be Noetherian. Then
\[ \hat{a} = \hat{A} \otimes_A a = a^\mathfrak{e} \]
This is the extended ideal. One of the easy basic properties of extended ideals which holds in complete generality is the statement
\[ (a^\mathfrak{e})^n = (a^n)^\mathfrak{e} \]
which proves (2).

Finally, we need to know that (6) $\Rightarrow$ (1). Take any $a \in \hat{a}$. Then
\[ (1 - a)^{-1} = 1 + a + a^2 + a^3 + \cdots \]
is a converging series. This is a Cauchy sequence in a complete ring and therefore converges. One can also see this by observing that this represents a compatible system of elements in the inverse system:
\[ \hat{A} = \lim_{\leftarrow} \hat{A}/\hat{a}^n : \]
\[ \cdots \to \hat{A}/\hat{a}^3 \to \hat{A}/\hat{a}^2 \to \hat{A}/\hat{a} \]
\[ 1 + a + a^2 + \hat{a}^3 \mapsto 1 + a + \hat{a}^2 \mapsto 1 + \hat{a} \]
This shows that
\[ 1 + \hat{a} \subseteq U(\hat{A}) \]
and this implies that $\hat{a} \subseteq Jrad(\hat{A})$.

**Corollary 10.25.** If $a = m$ is a maximal ideal in a Noetherian ring $A$ then $\hat{A}$ is a local ring with unique maximal ideal $\hat{m}$.

**Proof.** $\hat{A}/\hat{a} \cong A/m$ is a field. Therefore, $\hat{m}$ is a maximal ideal in $\hat{A}$. But $\hat{m} \subseteq Jrad(\hat{A})$. So, $\hat{m}$ is the unique maximal ideal.

10.3.2. **Krull’s theorem.** Krull found a formula for the kernel of the completion map $M \to \hat{M}$:

**Theorem 10.26.** If $A$ is Noetherian and $M$ is f.g. then
\[ \ker(M \to \hat{M}) = \bigcap a^n M = \{ x \in M \mid (1 + a)x = 0 \text{ for some } a \in a \} \]

**Proof.** ($\subseteq$) Let $E = \bigcap a^n M$. Then $aE = E$. Since $E \subseteq M$, $E$ is finitely generated. Therefore, by the determinant trick (Cor. 2.4), there exists an $a \in a$ so that $(1 + a)E = 0$.

($\supseteq$) Conversely, suppose that $(1 - a)x = 0$ for some $a \in a$. Then
\[ x = ax = a^2 x = a^3 x = \cdots \]
is an element of $E$.

**Corollary 10.27.** If $a \subseteq Jrad(A)$ then $M \subseteq \hat{M}$ (and $M$ is Hausdorff).
In particular, \( \hat{A} \) is Hausdorff since complete implies \( \hat{a} \subseteq Jrad(\hat{A}) \).

**Proof.** If \( a \subseteq Jrad(A) \) then \( 1 + a \subseteq U(A) \). So, \((1 + a)x = 0 \) implies \( x = 0 \). \( \square \)

**Corollary 10.28.** If \( A \) is a Noetherian domain then \( A \subseteq \hat{A} \).

**Corollary 10.29.** The ring \( A = C^\infty(\mathbb{R}) \) of \( C^\infty \) real valued functions on \( \mathbb{R} \) is not Noetherian.

**Proof.** Let \( a = \{ f \in A \mid f(0) = 0 \} \). Then I claim that \( a^n \) is the set of all functions \( f \) so that \( f(0) = f'(0) = f''(0) = \cdots = f^{(n-1)}(0) \), i.e., the value of \( f \) and its first \( n - 1 \) derivatives is zero at \( x = 0 \). To show this let

\[
g(x) = \int_0^1 f'(xt) \, dt
\]

Then \( g \) is a smooth function with \( g(0) = f'(0) \) and \( f(x) - f(0) = xg(x) \). The Leibnitz rule shows that any element of \( a^n \) satisfies the condition that the first \( n - 1 \) derivatives is zero. Conversely, if the first \( n - 1 \) derivatives of \( f \) at 0 is zero then the first \( n - 2 \) derivatives of \( g \) at 0 is zero. So, \( g \in a^{n-1} \) which implies that \( f = xg \in a^n \).

The intersection

\[
\bigcap a^n = \{ f \mid f(0) = 0 = f'(0) = f''(0) = \cdots \} \neq 0
\]

is nonzero since there are functions which are nonzero in a neighborhood of \( x \) all of whose derivatives vanish at 0.

But \((1 + a)f = 0 \) implies that \((1 + a(x))f(x) \neq 0 \) for \( x \) in a neighborhood of 0. This contradicts Krull’s criterion. So the ring cannot be Noetherian. \( \square \)

**10.3.3. properties of \( \text{Gr}(A) \).**

**Proposition 10.30.** Suppose that \( A \) is Noetherian.

1. \( \text{Gr}(A) \) is Noetherian.
2. If \( M \) is a f.g. \( A \)-module and \( (M_n) \) is a stable \( a \)-filtration of \( M \) then \( \text{Gr}(M) \) is a f.g. \( \text{Gr}(A) \)-module.

**Proof.** (1) Since \( A \) is Noetherian, \( a \) is finitely generated. So \( a/a^2 = (x_1, x_2, \cdots, x_n) \). Then \( a/a^2 = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n) \) where \( \overline{x}_i \) is the image of \( x_i \). But then

\[
\text{Gr}(A) = (A/a)[\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n]
\]

is Noetherian since it is the quotient of a Noetherian ring.

(2) \( (M_n) \) is stable iff \( \exists m_0 \) so that \( a^nM_{m_0} = M_{n+m_0} \) for all \( n \geq 0 \).

But this implies that

\[
(a^n/a^{n+1})M_{m_0}/M_{m_0+1} = M_{n+m_0}/M_{n+m_0+1}
\]
which implies that $\text{Gr}(M)$ is generated by $\bigoplus_{m \leq m_0} M_m/M_{m+1}$ and each $M_m/M_{m+1}$ is finitely generated being a subquotient of $M$. \hfill \square

Next we have what I called “Lemma 4” in the lecture:

**Proposition 10.31.** Suppose that $\phi : N \to M$ is a homomorphism so that $\phi(N_n) \subseteq M_n$ and let $\text{Gr}(\phi) : \text{Gr}(N) \to \text{Gr}(M)$ be the induced homomorphism of $\text{Gr}(A)$-modules and let $\hat{\phi} : \hat{N} \to \hat{M}$ be the induced homomorphism of $\hat{A}$-modules. Then

1. $\text{Gr}(\phi)$ mono implies $\hat{\phi}$ mono.
2. $\text{Gr}(\phi)$ onto implies $\hat{\phi}$ onto.

**Proof.** (1) Consider the following diagram where the rows are exact. Given that $\text{Gr}(\phi)$ is a monomorphism, then $\alpha$ is a monomorphism. Suppose by induction that $\gamma$ is a mono. Then the snake lemma gives us that $\beta$ is mono. So $\gamma$ is mono for all $n$. So, we get a monomorphism in the inverse limit: $\hat{N} \hookrightarrow \hat{M}$.

\[
\begin{array}{cccccc}
0 & \to & N_n/N_{n+1} & \to & N/N_{n+1} & \to & N/N_n & \to & 0 \\
& & \downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} & & \\
0 & \to & M_n/M_{n+1} & \to & M/M_{n+1} & \to & M/M_n & \to & 0
\end{array}
\]

(2) Suppose that $\text{Gr}(\phi)$ is onto. Then $\alpha$ is onto. Suppose by induction that $\gamma$ is onto. Then $\beta$ is onto. So, $\gamma$ is onto for all $n$. The snake lemma also says that $\ker \beta$ goes onto $\ker \gamma$. Therefore, the kernels form a surjective system with $\lim^1 = 0$. So, the induced map on inverse limits $\hat{N} \to \hat{M}$ is onto. \hfill \square

10.3.4. *Proof that $\hat{A}$ is Noetherian.* Here is the outline of the proof:

\[
\begin{align*}
\text{A Noetherian} & \Rightarrow \text{Gr}(A) \text{ Noetherian} \\
\| & \\
\hat{A} \text{ Noetherian} & \Leftarrow \text{Gr}(\hat{A}) \text{ Noetherian}
\end{align*}
\]

We just proved that $\text{Gr}(A)$ is Noetherian and we know $\text{Gr}(A) = \text{Gr}(\hat{A})$. So, it remains to prove the bottom implication. But we showed that $\hat{A}$ is complete. So, it suffices to prove the following.

**Lemma 10.32.** If $A$ is complete in the $a$-adic topology and $\text{Gr}(A)$ is Noetherian then $A$ is Noetherian.

Clearly, this lemma is all we need to finish the proof that $\hat{A}$ is Noetherian. But, Lemma 10.32 follows immediately from the next lemma applied to $M = A$. 

Lemma 10.33. Suppose $A$ is complete and $M$ is Hausdorff ($\bigcap M_n = 0$). Suppose $\text{Gr}(M)$ is a Noetherian $\text{Gr}(A)$-modules (i.e., every submodule is finitely generated). Then $M$ is Noetherian.

To prove this we need another lemma:

Lemma 10.34. Suppose that $A$ is complete and $M$ is Hausdorff. Suppose also that $\text{Gr}(M)$ is a f.g. $\text{Gr}(A)$-module. Then $M$ is a f.g. $A$-module.

Suppose first that this is true. Then we use it to prove Lemma 10.33.

Proof of Lemma 10.33. Suppose that $N \subseteq M$. Then define an $a$-filtration of $N$ by

$$N_n = N \cap M_n$$

This is the kernel of the map $N \to M/M_n$ so we get an exact sequence:

$$0 \to N/N_n \to M/M_n \to \frac{M}{N + M_n} \to 0$$

Compare this with:

$$0 \to N/N_{n+1} \to M/M_{n+1} \to \frac{M}{N + M_{n+1}} \to 0$$

We get vertical maps which are all onto. Therefore, we get a short exact sequence of kernels:

$$0 \to N_n/N_{n+1} \to M_n/M_{n+1} \to X \to 0$$

In other words, $\text{Gr}(N) \subseteq \text{Gr}(M)$. If $\text{Gr}(M)$ is Noetherian then $\text{Gr}(N)$ is f.g. Since $\bigcap N_n \subseteq N \cap \bigcap M_n = 0$, $N$ is also Hausdorff. So, $N$ is f.g. by Lemma 10.34. Since this holds for all $N \subseteq M$, this shows that $M$ is Noetherian. □

So, it remains to prove Lemma 10.34.

Proof of 10.34. We are given that $\text{Gr}(M)$ is a f.g. $\text{Gr}(A)$-module. Choose a finite set of homogeneous generators $x_i \in M_{n(i)}/M_{n(i)+1}$. Multiplication by $x_i$ induces mappings:

$$a^n/a^{n+1} \to M_{n+n(i)}/M_{n+n(i)+1}$$

which gives a homomorphism $\text{Gr}(A) \to \text{Gr}(M)$ of degree $n(i)$. If we shift $\text{Gr}(A)$ we can make this map have degree 0.

Let $\Sigma M$ be the shifted filtration of $M$ given by

$$\Sigma M_n = M_{n-1}$$

Then multiplication by $x_i$ gives a degree 0 homomorphism

$$\text{Gr}(\Sigma^{n(i)}) \to \text{Gr}(M)$$
We add these together using the notation $F^i = \Sigma^{n(i)} A$:

$$\sum x_i : \bigoplus Gr(F^i) \rightarrow Gr(M)$$

To say that the $x_i$ generate $Gr(M)$ as a $Gr(A)$ module is the same as saying that this map is onto.

By Proposition [10.31] this implies that the induced map on completions is surjective:

$$\bigoplus \widehat{F^i} \twoheadrightarrow \widehat{M}$$

But $\widehat{F^i} \cong \widehat{A} = A$ since $A$ is complete. This gives $\bigoplus A \rightarrow \widehat{M}$. So, $\widehat{M}$ is f.g.. Since $M$ is Hausdorff we have a monomorphism $g : M \hookrightarrow \widehat{M}$.

Now consider the following diagram:

$$
\begin{array}{ccc}
\bigoplus A & \xrightarrow{f} & M \\
\downarrow & & \downarrow g \\
\bigoplus \widehat{A^n} & \xrightarrow{\widehat{\phi}} & \widehat{M}
\end{array}
$$

Since $\widehat{\phi}$ is an epimorphism and $g$ is a monomorphism we conclude that $f$ is an epimorphism. Therefore, $M$ is finitely generated as claimed. □
11. Dimension theory

The dimension of a Noetherian local ring can be defined in several ways. The main theorem is that all of these descriptions give the same number. So far we have the Krull dimension \( \dim A \) which is the length of the maximal chain of prime ideals.

11.1. Poincaré series and Hilbert functions. Suppose that \( m \) is a maximal ideal of \( A \) and

\[
Gr(A) = \bigoplus A_n = A/m \oplus m/m^2 \oplus m^2/m^3 \oplus \cdots
\]

is the associated graded ring. If \( A \) is Noetherian then each \( A_n = m^n/m^{n+1} \) is a finite dimensional vector space over the field \( k = A_0 = A/m \) and we have the Poincaré series

\[
P_{Gr(A)}(t) = \sum_{n=0}^{\infty} t^n \dim_k A_n
\]

11.1.1. length function. In greater generality we consider a graded ring

\[
A = \bigoplus_{n=0}^{\infty} A_n = A_0 \oplus A_1 \oplus A_2 \oplus \cdots
\]

so that \( A \) is Noetherian and \( A_0 \) is Artinian. Suppose that

\[
M = \bigoplus_{n=0}^{\infty} M_n = M_0 \oplus M_1 \oplus M_2 \oplus \cdots
\]

is a finitely generated graded module over \( A \). Then each \( M_n \) is a finitely generated \( A_0 \)-module. Since \( A_0 \) is Artinian, each \( M_n \) has finite length \( \ell(M_n) \) and we can define the Poincaré series of \( M \) to be

\[
P_M(t) = \sum_{n=0}^{\infty} \ell(M_n)t^n
\]

Recall that the length of an \( A_0 \)-module \( N \) is defined to be the largest integer \( m = \ell(N) \) so that there is a filtration

\[
N = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_m = 0
\]

by \( A_0 \)-submodules \( N_n \). It can be shown that any two maximal filtrations have the same length. The subquotients \( N_n/N_{n+1} \) are called composition factors of \( N \). They are simple modules which are unique up to isomorphism and permutation of indices.

Given this property it is easy to see that the length function satisfies the property that, for any short exact sequence of f.g. \( A_0 \)-modules

\[
0 \to M' \to M \to M'' \to 0
\]
we have $\ell(M) = \ell(M') + \ell(M'')$. Any function on f.g. $A_0$-modules with this property is called an *additive function*.

Some trivial observations about the Poincaré series:

1. $0 \leq P_M(1) \leq \infty$ in general.
2. $P_M(1) = \sum \ell(M_n) < \infty$ iff $M_n = 0$ for all but finitely many $n$.
   (We are given that $\ell(M_n) < \infty$ for all $n \geq 0$.)
3. $P_M(1) = 0$ iff $M = 0$.

### 11.1.2. rational functions

**Theorem 11.1.** The Poincaré series of $M$ is a rational function of the form

$$P_M(t) = \frac{f(t)}{\prod_{i=1}^{s}(1 - t^{k_i})}$$

where $f(t)$ is a polynomial in $t$ with coefficients in $\mathbb{Z}$.

**Proof.** The proof is by induction on $s$, the number of homogeneous generators $x_i$ of the ideal $A_+$. 

If $s = 0$ then $A = A_0$ and each $M_n$ is an $A$-submodule of $M$. Since $M$ is f.g. this implies that $M_n = 0$ for all but finitely many $n$. So $P_M(t) = f(t) = \sum \ell(M_n)t^n$ is a polynomial in $t$ with coefficients in $\mathbb{Z}$.

Now suppose that $s \geq 1$ and consider the last generator $x_s \in A_{k_s}$. Multiplication by $x_s$ gives a graded map $M \to M$ of degree $k_s$. Let $K$ be the kernel and $L$ the cokernel of this map. Then, for each $n \geq 0$ we get an exact sequence:

$$0 \to K_{n-k_s} \to M_{n-k_s} \xrightarrow{x_s} M_n \to L_n \to 0$$

where $K_{n-k_s} = M_{n-k_s} = 0$ for $n < k_s$. Then

$$\ell(K_{n-k_s}) - \ell(M_{n-k_s}) + \ell(M_n) - \ell(L_n) = 0$$

Multiply by $t^n$

$$\ell(K_{n-k_s})t^n - \ell(M_{n-k_s})t^n + \ell(M_n)t^n - \ell(L_n)t^n = 0$$

Sum over all $n$

$$t^{k_s}P_K(t) - t^{k_s}P_M(t) + P_M(t) - P_L(t) = 0$$

So:

$$P_M(t) = \frac{P_L(t) - t^{k_s}P_K(t)}{1 - t^{k_s}}$$

Since $x_s$ annihilates $K$ and $L$, these are graded modules over the graded ring $\overline{A} = A/(x_s)$ whose positive grade ideal has $s - 1$ generators $\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_{s-1}$, the images of $x_i \in A$. So, $P_L(t)$ and $P_K(t)$ are rational functions with denominator $\prod_{i=1}^{s-1}(1 - t^{k_i})$. The theorem follows. \[\square\]
There is one special case when we can easily calculate \( f(t) \) by induction. This is the case in which \( K = 0 \), i.e., \( x_s z \neq 0 \) for all \( z \neq 0 \) in \( M \). In this case we say that \( x_s \) is \( M \)-regular. Then

\[
P_M(t) = \frac{P_{M/x_sM}(t)}{1 - tk_s}
\]

Next, suppose that \( x_s - 1 \) is \( M/x_sM \)-regular. Then

\[
P_{M/x_sM}(t) = \frac{P_{M/x_s-1x_sM}(t)}{1 - tk_{s-1}}
\]

**Definition 11.2.** We say that (any sequence of elements of \( A \)) \( x_k, \ldots, x_s \) is an \( M \)-regular sequence if this continues in the analogous way up to \( x_k \). When \( M = A \), we call this a regular sequence for \( A \).

By induction we would get:

\[
P_M(t) = \frac{P_{M/x_kx_{k+1} \ldots x_sM}(t)}{\prod_{i=k}^{s-1}(1 - tk_i)}
\]

**Example 11.3.** Take \( A = M = K[x_1, \ldots, x_d] \) graded in the usual way so that \( x_1, \ldots, x_d \) span \( A_1 = M_1 \). Then \( x_1, \ldots, x_d \) is an \( M \)-regular sequence and \( M/x_1 \ldots x_dM = K \) is 1-dimensional and

\[
P_A(t) = \frac{1}{(1 - t)^d} = \sum \binom{n + d - 1}{d - 1} t^n
\]

**Proof.** (of the second equality) Start with

\[
(1 - t)^{-1} = \sum t^n = 1 + t + t^2 + t^3 + \cdots
\]

and differentiate \( d - 1 \) times to get

\[
(d - 1)!(1 - t)^{-d} = \sum n(n - 1) \cdots (n - d + 2)t^{n-d+1}
\]

\[
(1 - t)^{-d} = \sum \binom{n}{d - 1} t^{n-d+1} = \sum \binom{n + d - 1}{d - 1} t^n
\]

\[
= \sum_{n=0}^{\infty} \left[ \frac{n^{d-1}}{(d - 1)!} - \frac{n^{d-2}}{(d - 3)!} + \cdots \right] t^n
\]

\[
\square
\]

11.1.3. dimension using \( P_M(t) \).

**Definition 11.4.** Let \( d = d(M) \) be the smallest positive integer so that

\[
\lim_{t \to 1} (1 - t)^d P_M(t) < \infty
\]

**Proposition 11.5.** \( d(M) \leq s \) for all f.g. graded \( A \)-modules \( M \).
Proof. 
\[
\frac{1 - t}{1 - t^k} = \frac{1}{1 + t + \cdots + t^{k-1}} \rightarrow \frac{1}{k}
\]
as \(t \rightarrow 1\). So, \((1 - t)^sP_M(t)\) converges as \(t \rightarrow 1\). \(\square\)

Lemma 11.6. If \(x \in A_k\) is \(M\)-regular then \(d(M) = d(M/xM) + 1\).

Proposition 11.7. If \(A\) has an \(M\)-regular sequence of length \(r\) then \(d(M) \geq r\).

In Example 11.3 \(d = s = r\). So, \(d(K[x_1, \cdots, x_d]) = d\). The idea is that \(d(M)\) is the number of generators of \(A\) which act as independent variables on \(M\).

11.1.4. Hilbert function. The Hilbert function gives a formula for \(\ell(M_n)\) for large \(n\).

Theorem 11.8. Suppose that \(k_i = 1\) for \(i = 1, 2, \cdots, s\). Then \(\ell(M_n)\) is a polynomial of degree \(d(M) - 1\) for large \(n\).

Proof. By Theorem 11.1 we have:
\[
\sum \ell(M_n)t^n = \frac{f(t)}{(1 - t)^s}
\]
where \(f(t)\) is a polynomial. By definition of \(d = d(M)\) we have \(f(t) = (1 - t)^s - d g(t)\) where \(g(1) \neq 0\). So,
\[
\sum \ell(M_n)t^n = \frac{g(t)}{(1 - t)^d} = \sum \binom{n + d - 1}{d - 1} t^n g(t)
\]
Suppose that \(g(t) = \sum_{k=0}^{m} a_k t^k = a_0 + a_1 t + \cdots + a_m t^m\). Then
\[
\sum \ell(M_n)t^n = \sum_{k=0}^{m} \sum a_k \binom{n + d - 1}{d - 1} t^{n+k}
\]
When \(n \geq m\) we get
\[
\ell(M_n) = \sum_{k=0}^{m} a_k \binom{n - k + d - 1}{d - 1}
\]
(When \(n < m\) we take the sum over \(0 \leq k \leq n\).) Since the binomial coefficient is a polynomial in \(n\) of degree \(d - 1\) with leading coefficient \(1/(d - 1)!\) regardless of the value of \(k\), this formula for \(\ell(M_n)\) is a polynomial in \(n\) of degree \(d - 1\) with leading coefficient
\[
\frac{1}{(d - 1)!} \sum_{k=0}^{m} a_k = \frac{g(1)}{(d - 1)!} \neq 0
\]
\(\square\)
**Definition 11.9.** The **Hilbert function** of $M$ is the polynomial function

$$h_M(n) = \ell(M_n)$$

for sufficiently large $n$.

11.1.5. **Samuel function.** For each $n$ consider the finite sum:

$$g(n) = \ell(M_0) + \ell(M_1) + \cdots + \ell(M_{n-1}).$$

**Lemma 11.10.** $g(n)$ is a polynomial of degree $d(M)$ for sufficiently large $n$.

**Proof.** For $m > m_0$ we have

$$\ell(M_m) = h_M(m) = c_0 + c_1m + \cdots + c_{d-1}m^{d-1}$$

Therefore

$$g(n) = \sum_{m=0}^{n-1} h_M(m) + \text{const}$$

for $n > m_0$. But, anyone who has taught Calculus knows that $\sum_{m=0}^{n-1} m^k$ is a polynomial in $n$ of degree $k + 1$. The lemma follows. □

Suppose that $A$ is a Noetherian local ring with unique maximal ideal $m$ and quotient field $K = A/m$. Let $M$ be any f.g. $A$-module. For any $n$, $M/m^nM$ is a f.g. module over the Artin local ring $A/m^n$. Therefore it has a finite length:

$$\ell(M/m^nM) = \dim_K(M/mM \oplus mM/m^2M \oplus \cdots \oplus m^{n-1}M/m^nM)$$

**Proposition 11.11.** For sufficiently large $n$, $\ell(M/m^nM)$ is a polynomial in $n$ of degree $\leq s = \dim_K(m/m^2)$.

**Proof.** Take the associated graded ring

$$\text{Gr}(A) = A/m \oplus m/m^2 \oplus m^2/m^3 \oplus \cdots$$

has positive ideal $\text{Gr}(A)_+ = m/m^2 \oplus m^2/m^3 \oplus \cdots$ generated by $s$ elements of degree 1. The associated $\text{Gr}(A)$-module

$$\text{Gr}(M) = M/mM \oplus mM/m^2M \oplus \cdots$$

is a f.g. $\text{Gr}(A)$-module with $d(\text{Gr}(M)) \leq s$ by Proposition [11.5]. So, $\ell(M/m^nM)$ is a polynomial of degree $d(\text{Gr}(M)) \leq s$ for sufficiently large $n$ by the lemma above. □

**Definition 11.12.** The **Samuel function** for $M$ is defined to be the polynomial function given for large $n$ by:

$$\chi^M_m(n) = \ell(M/m^nM)$$

$$\deg \chi^M_m(n) = d(\text{Gr}(M)) \leq \dim_K(m/m^2)$$
11.2. **Noetherian local rings.** Suppose that \( A \) is a Noetherian local ring with maximal ideal \( \mathfrak{m} \). We will prove the *main theorem of dimension theory* which says:

\[
d(A) = \dim A = \delta(A)
\]

**Definition 11.13.** If \( A \) is a Noetherian ring \( \delta(A) \) is defined to be the smallest number of elements which can generate a proper ideal \( \mathfrak{q} \) so that \( A/\mathfrak{q} \) is Artinian. When \( A \) is Noetherian local, this is equivalent to saying that \( \mathfrak{q} \) is \( \mathfrak{m} \)-primary. If \( M \) is a f.g. \( A \)-module we define \( \delta(M) \) to be \( \delta(A/\text{Ann}(M)) \).

Once we review the definition of \( d(A) \) we will see that we have already proven that

\[
d(A) \leq \delta(A)
\]

11.2.1. **definition of \( d(M) \).** Suppose that \( s = \delta(A) \) and \( \mathfrak{q} \) is an \( \mathfrak{m} \)-primary ideal generated by \( s \) elements. Then

\[
Gr_\mathfrak{q}(A) = A/\mathfrak{q} \oplus \mathfrak{q}/\mathfrak{q}^2 \oplus \mathfrak{q}^2/\mathfrak{q}^3 \oplus \cdots
\]

is a graded Noetherian local ring whose positive ideal \( Gr_\mathfrak{q}(A)_+ = \mathfrak{q}/\mathfrak{q}^2 \oplus \mathfrak{q}^2/\mathfrak{q}^3 \oplus \cdots \) is generated by \( s \) homogeneous elements in degree 1. Suppose that \( M \) is a f.g. \( A \)-module and \((M_n)\) is a stable \( \mathfrak{q} \)-filtration. Then

\[
Gr(M) = M/M_1 \oplus M_1/M_2 \oplus M_2/M_3 \oplus \cdots
\]

is a f.g. \( Gr_\mathfrak{q}(A) \)-module. This implies that the *Poincaré series*

\[
P_M(t) = \sum_{n=0}^{\infty} \ell(M_n/M_{n+1})t^n = \frac{f(t)}{(1-t)^s}
\]

where \( f(t) \in \mathbb{Z}[t] \). If we reduce the fraction we get \((1-t)^d\) in the denominator where \( d = d(M) \). So, clearly \( d \leq s = \delta(A) \). Replacing \( A \) with \( A/\text{Ann} M \) we get

\[
d(M) \leq \delta(M)
\]

(in particular \( d(A) \leq \delta(A) \)) with one particular definition of \( d(M) \).

Next recall that

\[
h(n) = \ell(M_n/M_{n+1})
\]

is a polynomial in \( n \) of degree \( d(M) - 1 \) for large \( n \). This was called the *Hilbert function* of \( M \). As a formal consequence of this theorem we concluded that, for large \( n \),

\[
g(n) = \ell(M/M_n)
\]
is a polynomial in $n$ of degree $d(M)$. (The theorem was stated only in
the case $M_n = m^n M$ but the same proof works for any filtration.) In
the particular case $M_n = q^n M$ we have the Samuel function
\[ \chi^M_q(n) = \ell(M/q^n M) \]

11.2.2. $d(M)$ is well defined. We will show that $d(M)$ is independent
of the choice of $q$ and the choice of the filtration $(M_n)$.

**Proposition 11.14.** Given any $m$-primary ideal $q$ and any stable $q$-
filtration $(M_n)$, the polynomials $g(n) = \ell(M/M_n)$ and $\chi^M_q(n) = \ell(M/q^n M)$
have the same degree and leading coefficient. Furthermore, this leading
coefficient is a positive rational number.

**Proof.** $(M_n)$ being $q$-stable means $\exists n_0$ s.t.
\[ q^{n+n_0} M \subseteq M_{n+n_0} = q^n M_{n_0} \subseteq q^n M \]
This implies that
\[ \ell(M/q^{n+n_0}) \geq \ell(M/M_{n+n_0}) \geq \ell(M/q^n M) \]
\[ \chi^M_q(n+n_0) \geq g(n+n_0) \geq \chi^M_q(n) \]
But $\chi^M_q(n+n_0)$ and $\chi^M_q(n)$ are polynomials in $n$ of the same degree and
the same leading coefficient. So, $g(n+n_0) = \ell(M/M_{n+n_0})$ and therefore $g(n)$ also has the same degree and leading coefficient. Positivity is
obvious. \Box

**Proposition 11.15.** The degree of the polynomial $\chi^M_q(n)$ is independent
of the choice of the $m$-primary ideal $q$.

**Proof.** If $q$ is $m$-primary then $m^a \subseteq q \subseteq m$ for some $a$. This implies
$m^{na} \subseteq q^n \subseteq m^n$ which implies
\[ \ell(M/m^{na} M) \geq \ell(M/q^n M) \geq \ell(M/m^n M) \]
\[ \chi^M_m(na) \geq \chi^M_q(n) \geq \chi^M_m(n) \]
But it is easy to see that $\chi^M_m(na)$ is a polynomial in $n$ with the same
degree, say $d$, as $\chi^M_m(n)$ (with leading coefficient multiplied by $a^d$). So,
$\chi^M_q(n)$ is a polynomial of degree $d$ in $n$. \Box

**Theorem 11.16.** If $A$ is a Noetherian local ring and $M$ is a finitely
generated $A$-module then $d(M) \leq \delta(M)$. In particular
\[ d(A) \leq \delta(A). \]
11.2.3. Krull dimension. The plan is to prove that
\[ \delta(A) \geq d(A) \geq \dim A \geq \delta(A) \]
showing that all three are equal. We discussed the definitions of the first two terms and proved the first inequality. Now we prove the second. The proof will be by induction on \( d(A) \) (we have not yet proven that \( \dim A \) is finite).

**Lemma 11.17.** If \( 0 \to M' \to M \to M'' \to 0 \) is a short exact sequence of \( A \)-modules then
\[ d(M) = \max(d(M'), d(M'')) \]
Furthermore, if \( M \cong M' \) then \( d(M) > d(M'') \).

**Proof.** For each \( n \) we have the short exact sequence:
\[ 0 \to M' \cap m^nM \to m^nM \to m^nM'' \to 0 \]
By the Artin-Rees Lemma, \( (M' \cap m^nM) \) is a stable \( m \)-filtration of \( M' \). This exact sequence gives an exact sequence of quotient modules
\[ 0 \to \frac{M'}{M' \cap m^nM} \to \frac{M}{m^nM} \to \frac{M''}{m^nM''} \to 0 \]
Since length is additive, this gives
\[ \ell \left( \frac{M}{m^nM} \right) = \ell \left( \frac{M'}{M' \cap m^nM} \right) + \ell \left( \frac{M''}{m^nM''} \right) \]
\[ \chi_M^m(n) = g(n) + \chi_{M''}^m(n) \]
By Proposition 11.14, the polynomial \( g(n) \) has degree \( d(M') \) and \( \chi_M^m(n) \) has degree \( d(M'') \). Since both of these polynomials have positive leading terms, the leading terms cannot cancel and their sum has degree equal to the maximum of the two degrees.
In the special case when \( M \cong M' \), we use the fact that \( g(n) \) will have the same degree and the same leading coefficient as \( \chi_M^m(n) \) causing \( \chi_M^m(n) \) to have smaller degree. \( \square \)

**Theorem 11.18.** If \( A \) is a Noetherian local ring with Krull dimension \( \dim A \) then
\[ d(A) \geq \dim A \]

**Proof.** By induction on \( d(A) \). If \( d(A) = 0 \) then \( m^n = 0 \) for some \( n \) making \( A \) Artinian with \( \dim A = 0 \). So, suppose \( d = d(A) > 0 \) and the theorem holds for \( B \) with \( d(B) < d \).
We are trying to show that \( \dim A \leq d \). So, suppose by contradiction that \( \dim A > d \). Then there exists a tower of prime ideals in \( A \) of length \( d + 1 \):

\[
\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_{d+1}
\]

Choose any \( x \in \mathfrak{p}_1 - \mathfrak{p}_0 \). Let \( \overline{x} \) be the image of \( x \) in the integral domain \( A' = A/\mathfrak{p}_0 \). Then \( \overline{x} \) is \( A' \)-regular (not a unit and not a zero divisor). Therefore we have an exact sequence of \( A \)-modules

\[
0 \to A/\mathfrak{p}_0 \xrightarrow{x} A/\mathfrak{p}_0 \to A'/\overline{x} \to 0
\]

By the lemma,

\[
d = d(A) \geq d(A') > d(A'/\overline{x}) \geq d(A/\mathfrak{p}_1)
\]

By induction on \( d \) we have

\[
d(A/\mathfrak{p}_1) \geq \dim A/\mathfrak{p}_1 \geq d
\]

since \( \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_{d+1} \) gives a tower of prime ideals of length \( d \) in \( A/\mathfrak{p}_1 \). This is a contradiction proving the theorem.

\[ \square \]

11.2.4. the fundamental theorem of dimension theory.

**Theorem 11.19.** If \( A \) is a Noetherian local ring then

\[
\dim A \geq \delta(A)
\]

**Proof.** Let \( d = \dim A \).

Claim 1 \( \exists x_1, \cdots, x_d \in \mathfrak{m} \) so that

\[
\dim A/(x_1, \cdots, x_i) \leq d - i
\]

In particular, \( \dim A/(x_1, \cdots, x_d) = 0 \iff (x_1, \cdots, x_d) \) is \( \mathfrak{m} \)-primary \( \Rightarrow \delta(A) \leq d \). So, it suffices to prove this claim.

We prove Claim 1 by induction on \( d \). If \( d = 0 \) the statement is clearly true. So, suppose that \( d > 0 \).

Claim 2 If \( d = \dim A > 0 \) then \( \exists x_1 \in \mathfrak{m} \) so that

\[
\dim(A/(x_1)) < d
\]

By induction on \( i \), Claim 2 implies Claim 1. So, it suffices to prove Claim 2.

Since \( A \) is Noetherian, \( A \) contains only finitely many minimal primes. (They are the minimal primes associated to the primary ideals in the primary decomposition of \( 0 \).) Let \( \mathfrak{p}_1, \cdots, \mathfrak{p}_i \) be these minimal primes. Then

\[
\mathfrak{m} \supseteq \bigcup \mathfrak{p}_i
\]

(If \( \mathfrak{m} = \bigcup \mathfrak{p}_i \) then by prime avoidance we would have \( \mathfrak{m} \subseteq \mathfrak{p}_i \) for some \( i \) contradicting the assumption that \( \dim A > 0 \).)
Let \( x_1 \in m \) so that \( x \notin p_i \) for any \( i \). Then \( \dim(A/(x_1)) < d \) because, if not, there would be a tower of prime ideals in \( A/(x_1) \) of length \( d \). This would give a tower of prime ideals
\[
q_0 \subsetneq q_1 \subsetneq \cdots \subsetneq q_d
\]
in \( A \) all of which contain \((x_1)\). But \( x_1 \) is not contained in any minimal prime. So, \( q_0 \) is not minimal. So, the tower can be extended contradicting the hypothesis that \( \dim A = d \).

This proves Claim 2 which implies Claim 1 which proves the theorem.

\[ \square \]

**Corollary 11.20** (Fundamental theorem of dimension theory). If \( A \) is a Noetherian local ring then
\[
\dim A = d(A) = \delta(A)
\]

In particular, \( \dim A \) is finite.

**Corollary 11.21.** If \( A \) is a Noetherian local ring with maximal ideal \( m \) and \( k = A/m \) then
\[
\dim A \leq \dim_k m/m^2
\]

**Corollary 11.22.** In any Noetherian ring, every prime ideal has finite height. In particular, the prime ideals satisfy the DCC.
11.3. **regular local rings.** Suppose that $A$ is a Noetherian local ring of dimension $d$. Then there exist $d$ elements $x_1, \ldots, x_d$ in $A$ which generate an $m$-primary ideal $q$ in $A$. Such a collection of elements is called a **system of parameters** for $A$.

**Definition 11.23.** A system of parameters for $A$ is called **regular** if it generates the maximal ideal $m$. If $A$ has a regular system of parameters it is called a **regular local ring**.

11.3.1. **first characterization of regular local rings.**

**Proposition 11.24.** Suppose that $A$ is a Noetherian local ring with $\dim A = d$. Then the following are equivalent.

1. $Gr_m(A) \cong k[t_1, \ldots, t_d]$.
2. $\dim_k m/m^2 = d$.
3. $m$ is generated by $d$ elements.
4. $A$ is a regular local ring.

**Proof.** Certainly (1) $\Rightarrow$ (2) and (3) $\Leftrightarrow$ (4) by definition of regular local ring. Nakayama’s lemma implies that (2) $\Leftrightarrow$ (3). To show that (3) $\Rightarrow$ (1) suppose that $x_1, \ldots, x_d$ generate $m$, i.e., they form a regular system of parameters for $A$. Then we get an epimorphism of graded rings

$$\varphi : k[t] = k[t_1, \ldots, t_d] \to Gr_m(A)$$

sending $t_i$ to the image $\overline{x_i}$ of $x_i$ in $m/m^2$. If this homomorphism is not an isomorphism then it has a nonzero element in its kernel, say $f(t)$. But $k[t]$ is an integral domain. So, $f(t)$ is not a zero divisor. And it cannot be a unit, being in the kernel of $\varphi$. So $f$ is regular and thus

$$d(k[t_1, \ldots, t_d]/(f)) = d(k[t_1, \ldots, t_d]) - 1 = d - 1$$

But $Gr_m(A)$ is a quotient of $k[t_1, \ldots, t_d]/(f)$. So,

$$d = d(Gr_m(A)) \leq d(k[t_1, \ldots, t_d]/(f)) = d - 1$$

which is a contradiction. So, $\varphi$ must be an isomorphism as claimed. $\square$

**Corollary 11.25.** A regular local ring is an integral domain.

**Proof.** By Krull’s theorem [10.26], $\bigcap m^n = 0$. Therefore the following lemma applies. $\square$

**Lemma 11.26.** Suppose that $a$ is an ideal in $A$ so that $\bigcap a^n = 0$. Suppose that $Gr_a(A)$ is an integral domain. Then $A$ is an integral domain.
Proof. Suppose that \( x, y \) are nonzero elements of \( A \). Since \( \bigcap a^n = 0 \), \( x \in a^n, x \notin a^{n+1} \) for some \( n \geq 0 \) and similarly \( y \in a^m, y \notin a^{m+1} \) for some \( m \geq 0 \). Then the images of these elements \( x \in a^n/a^{n+1} \), \( y \in a^m/a^{m+1} \) are nonzero in \( Gr_a(A) \) and therefore their product

\[
\bar{x} \bar{y} = \bar{xy} \in a^{n+m}/a^{n+m+1}
\]

is nonzero (since \( Gr_a(A) \) is an integral domain). This implies that \( xy \notin a^{n+m+1} \) and, in particular, \( xy \neq 0 \). \( \square \)

Corollary 11.27. A ring \( A \) is a regular local ring of dimension 1 iff it is a discrete valuation ring.

Proposition 11.28. Let \( A \) be a Noetherian local ring. Then \( \hat{A} \) is a Noetherian local ring with the same dimension and \( A \) is regular iff \( \hat{A} \) is regular.

11.3.2. Koszul complex. We will use the Koszul complex to prove part of the following well known theorem.

Theorem 11.29 (Serre). Suppose that \( A \) is a Noetherian local ring. Then the following are equivalent.

1. \( A \) is regular.
2. \( \text{gl} \dim A < \infty \)
3. \( \text{gl} \dim A = \dim A \)

Suppose that \( x_1, \ldots, x_d \in A \). Then the Koszul complex \( K_*(x_1, \ldots, x_d) \) is the chain complex of f.g. free \( A \) modules given by:

\[
K_n(x) = \text{free } A\text{-module generated by } e_{i_1i_2\cdots i_n} \cong A^{(d)}
\]

where \( 1 \leq i_1 < i_2 < \cdots < i_n \leq d \) with differential \( \partial : K_n \to K_{n-1} \) given by

\[
\partial(e_{i_1i_2\cdots i_n}) = \sum_{j=1}^{n} (-1)^{j+1} x_{i_j} e_{i_1\cdots \hat{i}_j\cdots i_n}
\]

It is easy to see that \( \partial \partial = 0 \). Also \( 0 \leq n \leq d \):

\[
0 \to K_d(x) \xrightarrow{\partial_d} K_{d-1}(x) \to \cdots \to K_1(x) \xrightarrow{\partial_1} K_0(x) \to K_0(x) = A.
\]

Claim: \( K_0(x) = A \) and the image of \( \partial_1 : K_1(x) \to A = K_0(x) \) is the ideal \( \mathfrak{q} = (x_1, \ldots, x_d) \). So the Koszul complex is augmented over \( A/\mathfrak{q} \):

\[
0 \to K_d(x) \xrightarrow{\partial_d} K_{d-1}(x) \to \cdots \to K_1(x) \xrightarrow{\partial_1} K_0(x) \xrightarrow{\epsilon} A/\mathfrak{q} \to 0
\]

Lemma 11.30. If \( A \) is a regular local ring of \( \dim A = d \) and \( x_1, \ldots, x_d \) is a regular system of parameters for \( A \) then the Koszul complex \( K_*(x) \) is a free resolution of \( k = A/\mathfrak{m} \).
We went over the basic definitions in class. The global dimension of a ring is the supremum of the projective dimensions of all f.g. modules. This is defined in terms of projective modules.

**Definition 11.31.** A module $P$ is projective if it satisfies the property that for any epimorphism of modules $p : X \rightarrow Y$ and any homomorphism $f : P \rightarrow Y$ there exists a morphism $\tilde{f} : P \rightarrow X$ so that $f = p \circ \tilde{f}$.

\[
\begin{array}{c}
X \\
\downarrow \quad \downarrow \quad \downarrow \\
\exists \tilde{f} \\
P \\
\downarrow \\
Y
\end{array}
\]

If we take $X = A^n$ and $Y = P$ with $f = id_P$, we get the following characterization of projective modules.

**Proposition 11.32.** A module $P$ is projective iff it is isomorphic to a direct summand of a free module. Every f.g. projective module is isomorphic to a direct summand of $A^n$ for some positive integer $n$.

**Definition 11.33.** The projective dimension $pd \dim M$ of any $A$-module $M$ is defined to be the smallest integer $n$ so that there exists an exact sequence:

$$0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \overset{\epsilon}{\rightarrow} M \rightarrow 0$$

where the $P_i$ are all projective modules.

In class I “rotated” the augmentation map $\epsilon : P_0 \rightarrow M$ to get the following diagram:

$$\begin{array}{c}
P_\ast : \\
\begin{array}{c}
0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \overset{\epsilon}{\rightarrow} M \rightarrow 0
\end{array}
\end{array}$$

$$\begin{array}{c}
M : \\
\begin{array}{c}
\cdots \rightarrow 0 \rightarrow M \rightarrow 0
\end{array}
\end{array}$$

The exactness of the original sequence is equivalent to the statement that $\epsilon$ is a quasi-isomorphism of chain complexes.

**Definition 11.34.** A quasi-isomorphism of chain complexes is defined to be a chain map which induces an isomorphism in homology in all degrees.

In the case at hand, the projective chain complex $P_\ast$ is exact except in degree 0 where the map $P_1 \rightarrow P_0$ is not onto. So, $H_0(P_\ast) \cong M$ and $\epsilon : P_0 \rightarrow M$ gives a quasi-isomorphism $P_\ast \simeq M$.

**Definition 11.35.** The global dimension of any ring $A$ is defined to be the supremum of $pf \dim M$ for all f.g. $A$-modules $M$. 
Lemma 11.30 (proved below) implies that \( \text{pr dim}_A k \leq d \). We need to strengthen this to an equality and then we need another lemma:

**Lemma 11.36.** If \( A \) is a local ring with maximal ideal \( \mathfrak{m} \) and \( k = A/\mathfrak{m} \) then

\[
\text{gl dim } A = \text{pr dim } k.
\]

**Proof.** By definition of global dimension we have \( \text{gl dim } A \geq \text{pr dim } k \). So, we need to show the reverse inequality. Suppose that \( \text{pr dim } M = n \). Then there is a projective complex

\[
0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to 0
\]

which is quasi-isomorphic to \( M \). Tor\(_A^n(M, k) \) is the kernel of the mapping

\[
P_n \otimes k \to P_{n-1} \otimes k
\]

But this mapping is 0 by Nakayama (assuming the projective complex \( P_* \) is minimal). So, \( \text{Tor}_A^n(M, k) \neq 0 \). But

\[
\text{Tor}_A^n(k, M) \cong \text{Tor}_A^n(M, k)
\]

So, this implies that \( \text{pr dim } k \geq n \). Therefore,

\[
\text{pr dim } M \leq \text{pr dim } k
\]

for all f.g. \( A \)-modules \( M \). The lemma follows. \( \square \)

We need another lemma to do the induction step for the proof that the Koszul complex is exact.

**Lemma 11.37.** If \( x_1, \cdots, x_d \) is a regular system of parameters for a regular local ring \( A \) then \( A/(x_1, \cdots, x_n) \) is a regular local ring of dimension \( d - n \) for \( n = 1, 2, \cdots, d \).

**Proof.** By induction it suffices to do the case \( n = 1 \). In that case, \( x_1 \) is a regular element since \( A \) is an integral domain. So, \( \dim A/(x_1) = d - 1 \). But the images \( \bar{x}_2, \cdots, \bar{x}_d \) of \( x_2, \cdots, x_d \) generate the maximal ideal of \( A/(x_1) \). So, \( A/(x_1) \) is regular. \( \square \)

**Proof of Lemma 11.30.** The proof is by induction on the length of the regular sequence. The induction hypothesis is:

**Claim:** For all \( 1 \leq n \leq d \), the Koszul complex \( K_*(x_1, \cdots, x_n) \) is quasi-isomorphic to \( A/(x_1, \cdots, x_n) \).

For \( n = d \) this is the statement that we want to prove.

Start with \( n = 1 \). Since \( x_1 \) is regular, multiplication by \( x_1 \) is a monomorphism and we have an exact sequence:

\[
0 \to A \xrightarrow{x_1} A \to A/(x_1) \to 0
\]
When we “rotate” the augmentation map this becomes a quasi-isomorphism
\( K_s(x_1) \simeq A/(x_1) \). So, the Claim holds for \( n = 1 \).

The case \( n = 2 \) shows the idea of the induction step. In this case the Koszul complex \( K_s(x_1, x_2) \) looks like:

\[
\begin{array}{c}
\overset{x_2}{-} \quad \overset{x_1}{-} \\
\overset{x_1}{+} \quad \overset{x_2}{+} \\
\overset{x_1}{-} \quad \overset{x_2}{-}
\end{array}
\]

This complex contains two copies of the smaller complex \( K_s(x_1) \) one is shifted and the boundary map from one copy to the other is multiplication by \( x_2 \). This means we have a short exact sequence of chain complexes:

\[
0 \to K_s(x_1) \to K_s(x_1, x_2) \to \Sigma K_s(x_1) \to 0
\]

We know by induction that \( K_s(x_1) \simeq A/(x_1) \). So, we can compare this to the complex:

\[
0 \to A/(x_1) \to X_* \to \Sigma A/(x_1) \to 0
\]

where \( X_* \) is the chain complex:

\[
X_* : A/(x_1) \xrightarrow{x_2} A/(x_1)
\]

This is the Koszul complex \( K_s(x_2) \) for the regular local ring \( A/(x_1) \). So, it is quasi-isomorphic to \( A/(x_1, x_2) \). We have the following commuting diagram where the rows are exact and the first and third vertical maps are quasi-isomorphisms by induction. So, the middle vertical arrow is also a quasi-isomorphism by the 5-lemma.

\[
\begin{array}{c}
0 \quad \longrightarrow \quad K_s(x_1) \quad \longrightarrow \quad K_s(x_1, x_2) \quad \longrightarrow \quad \Sigma K_s(x_1) \quad \longrightarrow \quad 0 \\
\downarrow \simeq \quad \downarrow \simeq \quad \downarrow \simeq \\
0 \quad \longrightarrow \quad A/(x_1) \quad \longrightarrow \quad X_* \quad \longrightarrow \quad \Sigma A/(x_1) \quad \longrightarrow \quad 0
\end{array}
\]

Therefore

\[
K_s(x_1, x_2) \simeq X_* \simeq A/(x_1, x_2).
\]

The next steps are similar. \( \square \)

11.3.3. \textit{multiplicity.} I gave a very brief summary of another use for the Koszul complex. Namely, in the equation for the leading terms of the Samuel function

\[
\chi^A_q(n) = \ell(A/q^n)
\]
Theorem 11.38. Suppose that $A$ is a Noetherian local ring of dimension $d$ and $x_1, \ldots, x_d$ is a system of parameters for $A$. Let $q = (x_1, \ldots, x_d)$. Then the leading term of the Samuel function $\chi_q^A(n)$ is equal to

$$\frac{\chi(K_*(x_1, \ldots, x_d))}{d!} t^d$$

where $\chi(K_*(x))$ is the Euler characteristic of the Koszul complex:

$$\chi(K_*(x)) = \sum_{i=0}^{d} (-1)^i \ell(H_i(K_*(x)))$$

For example in the case of a regular local ring the leading term is

$$\frac{1}{d!} t^d$$

and

$$H_i(K(x)) = \begin{cases} k & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases}$$