MATH 603: INTRODUCTION TO COMMUTATIVE ALGEBRA

THOMAS J. HAINES

1. Lecture 1

1.1. **What is this course about?** The foundations of differential geometry (= study of manifolds) rely on analysis in several variables as "local machinery": many global theorems about manifolds are reduced down to statements about what happens in a local neighborhood, and then anaylsis is brought in to solve the local problem.

Analogously, algebraic geometry uses commutative algebraic as its "local machinery". Our goal is to study commutative algebra and some topics in algebraic geometry in a parallel manner. For a (somewhat) complete list of topics we plan to cover, see the course syllabus on the course web-page.

1.2. **References.** See the course syllabus for a list of books you might want to consult. There is no required text, as these lecture notes should serve as a text. They will be written up "in real time" as the course progresses. Of course, I will be grateful if you point out any typos you find.

In addition, each time you are the first person to point out any real mathematical inaccuracy (not a typo), I will pay you 10 dollars!!

1.3. **Conventions.** Unless otherwise indicated in specific instances, all rings in this course are commutative with identity element, denoted by 1 or sometimes by e. We will assume familiarity with the notions of homomorphism, ideal, kernels, quotients, modules, etc. (at least).

We will use Zorn's lemma (which is equivalent to the axiom of choice): Let $S, \leq$ be any non-empty partially ordered set. A *chain* T in S is a subset $T \subseteq S$ such that $x, y \in T$ implies $x \leq y$ or $y \leq x$ holds. If $S, \leq$ is such that every chain has an upper bound in S (an element $s \in S$ with $t \leq s$ for all $t \in T$), then S contains at least one maximal element.

1.4. **Correspondence between ideals and homomorphisms.** We call any surjective homomorphism $A \to B$ a *quotient*. We say the quotients $f_1 : A \to B_1$ and $f_2 : A \to B_2$ are *equivalent* if there exists a ring isomorphism $\phi : B_1 \xrightarrow{\sim} B_2$ satisfying $\phi \circ f_1 = f_2$.

The terminology is justified because any surjective homomorphism $f : A \to B$ is clearly equivalent to the canonical quotient $A \to A/\ker(f)$.

Proposition 1.4.1. (1) *There is an order-preserving correspondence*

$$\{\textit{ideals } I \subseteq A\} \longleftrightarrow \{\textit{equivalence classes of quotients } A \to B\}.$$

The correspondence sends an ideal I to the equivalence class of the canonical quotient $A \to A/I$, and the quotient $f : A \to B$ to the ideal $\ker(f) \subseteq A$.

Date: Fall 2005.

(2) *Fix an ideal $I \subset A$. There is an order-preserving correspondence*

$$\{\textit{ideals } J \subseteq A \textit{ containing } I\} \longleftrightarrow \{\textit{ideals of } A/I\},$$

given by: send an ideal $J \supset I$ to its image $\overline{J}$ in A/I, and send an ideal $J' \subseteq A/I$ to its pre-image under the canonical map $A \to A/I$.

1.5. **Prime and maximal ideals.** A *domain* is a ring A with the property: $1 \neq 0$ and if $x, y \in A$ and $xy = 0$, then $x = 0$ or $y = 0$. Examples are the integers $\mathbb{Z}$, and any ring of polynomial functions over a field.

An ideal $\mathfrak{p} \subset A$ is *prime* if it is proper ($\mathfrak{p} \neq A$) and $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is a domain.

An ideal $\mathfrak{m} \subset A$ is *maximal* if $\mathfrak{m} \neq A$ and there is no ideal I satisfying $\mathfrak{m} \subsetneq I \subsetneq A$. Equivalently, $\mathfrak{m}$ is maximal if and only $A/\mathfrak{m}$ is a field. To see this, check that any ring R having only (0) and R as ideals is a field. Now $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ has no ideals other than (0) and $A/\mathfrak{m}$ (Prop. 1.4.1), so the result follows on taking $R = A/\mathfrak{m}$ in the previous statement.

In particular, every maximal ideal is prime.

Proposition 1.5.1. *Maximal ideals exist in any ring A with $1 \neq 0$.*

Proof. This is a standard application of Zorn's lemma. Let S be the set of all proper ideals in A, ordered by inclusion. Let $T = \{I_\alpha\}_{\alpha \in \mathfrak{A}}$ be a chain of proper ideals. Then the union $\cup_{\alpha \in \mathfrak{A}} I_\alpha$ is an ideal which is an upper bound of T in S. Hence by Zorn's lemma S has maximal elements, and this is what we claimed. □

Let us define $\mathrm{Spec}(A)$ to be the set of all prime ideals of A, and $\mathrm{Spec}_{\mathfrak{m}}(A)$ to be the subset consisting of all maximal ideals. These are some of the main objects of study in this course. The nomenclature "spectrum" comes from functional analysis, and will be explained later on. Also, pretty soon we will give the set $\mathrm{Spec}(A)$ the structure of a topological space and discuss the foundations of algebraic geometry...

1.6. **Operations of contraction and extension.** Fix a homomorphism $\phi : A \to B$. For an ideal $I \subseteq A$ define its extension $I^e \subseteq B$ to the ideal generated by the image $\phi(I)$; equivalently, $I^e = \cap_J J$ where $J \subseteq B$ ranges over all ideals containing the set $\phi(I)$.

Dually, for an ideal $J \subseteq B$ define the contraction $J^c := \phi^{-1}(J)$, an ideal in A.

Note that J prime $\Rightarrow$ J^c prime, so contraction gives a map of sets $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$.

On the other hand, contraction does not preserve maximality: consider the contraction of $J = (0)$ under the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Therefore, a homomorphism $\phi : A \to B$ *does not* always induce a map of sets $\mathrm{Spec}_{\mathfrak{m}}(B) \to \mathrm{Spec}_{\mathfrak{m}}(A)$.

As we will see later on, there is a natural situation where ϕ *does* induce a map $\mathrm{Spec}_{\mathfrak{m}}(B) \to \mathrm{Spec}_{\mathfrak{m}}(A)$: this happens if A, B happen to be *finitely generated algebras over a field*. This is quite important and is a consequence of **Hilbert's Nullstellensatz**, one of the first important theorems we will cover.

1.7. **Nilradical.** Define the *nilradical* of A by

$$\mathrm{rad}(A) := \{f \in A \mid f^n = 0, \text{ for some } n \geq 1\}.$$

Check that $\mathrm{rad}(A)$ really is an ideal. Elements f satisfying the condition $f^n = 0$ for some $n \geq 1$ are called *nilpotent*.

Counterexample: For a non-commutative ring, it is no longer always true that the sum of two nilpotent elements is nilpotent. The elements $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, in the ring $M_2(R)$ over a ring R with $1 \neq 0$, are nilpotent, but their sum $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is not.

Lemma 1.7.1.

$$\mathrm{rad}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}.$$

Proof. The inclusion $\subseteq$ is clear from the definition of prime ideal. For the reverse inclusion, suppose $f \in A$ is not nilpotent, i.e., suppose $f^n \neq 0$ for every $n \geq 1$.

Let $\Sigma = \{I \mid f^n \notin I,\ \forall n \geq 1\}$. This set is non-empty (it contains the ideal $I = (0)$) and this set has a maximal element (Zorn). Call it $\mathfrak{p}$. We claim that $\mathfrak{p}$ is prime (and this is enough to prove $\supseteq$). If not, choose $x, y \notin \mathfrak{p}$ such that $xy \in \mathfrak{p}$. Since $\mathfrak{p} + (x) \supsetneq \mathfrak{p}$ and $\mathfrak{p} + (y) \supsetneq \mathfrak{p}$, we have $f^n \in \mathfrak{p} + (x)$ and $f^m \in \mathfrak{p} + (y)$ for some positive integers n, m. But then $f^{n+m} \in \mathfrak{p}$, a contradiction. □

1.8. **Radical of an ideal.** Define $r(I) = \{f \in A \mid f^n \in I, \text{ for some } n \geq 1\}$. Often, we denote $r(I) = \sqrt{I}$. Check that $\sqrt{I}$ is an ideal. Note that $\mathrm{rad}(A) = \sqrt{(0)}$. Also, it is easy to check the following fact:

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}. \tag{1.8.1}$$

Here $\mathfrak{p}$ ranges over prime ideals containing I.

1.9. **Jacobson radical.** Define the ideal $\mathrm{rad}_{\mathfrak{m}}(A) = \bigcap_{\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)} \mathfrak{m}$.

Proposition 1.9.1.

$$\mathrm{rad}_{\mathfrak{m}}(A) = \{x \in A \mid 1 - xy \text{ *is a unit for all* } y \in A\}.$$

Proof. $\subseteq$: Say $x \in \mathrm{rad}_{\mathfrak{m}}(A)$. If y is such that $1 - xy$ is not a unit, then $1 - xy \in \mathfrak{m}$, for some maximal ideal $\mathfrak{m}$. But then $1 \in \mathfrak{m}$, which is nonsense.

$\supseteq$: If $x \notin \mathfrak{m}$ for some $\mathfrak{m}$, then $(x) + \mathfrak{m} = A$. But then $1 = z + xy$, for some $z \in \mathfrak{m}$ and $y \in A$. So $1 - xy$ is not a unit. □

Exercise 1.9.2. *Prove the following statements.*

(i) $r(r(I)) = r(I)$;
(ii) $\mathrm{rad}(A/\mathrm{rad}(A)) = 0$;
(iii) $\mathrm{rad}_{\mathfrak{m}}(A/\mathrm{rad}_{\mathfrak{m}}(A)) = 0$.

We call an ideal I *radical* if $r(I) = I$. So, (i) shows that the radical ideals are precisely those of the form $r(I)$, for some ideal I.

There exist ideals which are not radical. Consider $(X^2) \subset \mathbb{C}[X]$, and note that $r(X^2) = (X)$.

Both $\mathrm{rad}(A)$ and $\mathrm{rad}_{\mathfrak{m}}(A)$ have some meaning in algebraic geometry, which we will return to shortly. Also, we will see that radical ideals play an important role too.

1.10. **Modules.** Let M be an abelian group. Then the ring of group endomorphisms of M, denoted $\mathrm{End}(M)$, is a ring (in general non-commutative). Giving M the structure of an A-module is precisely the same thing as giving a ring homomorphism

$$A \to \mathrm{End}(M).$$

We have correspondences as in Prop. 1.4.1

$$\{\text{submodules } N \subseteq M\} \longleftrightarrow \{\text{quotients } M \to M'\}$$

and

$$\{\text{submodules } N' \subseteq M \text{ containing } N\} \longleftrightarrow \{\text{submodules of } M/N\}.$$

Also, we have the fundamental isomorphisms of A-modules

(i) If $N, N' \subseteq M$, then $\dfrac{N+N'}{N} \cong \dfrac{N'}{N \cap N'}$;

(ii) If $N' \subseteq N \subseteq M$, then $\dfrac{M/N'}{N/N'} \cong M/N$.

1.11. **NAK Lemmas.** These lemmas are collectively called the Nakayama (or Nakayama-Azumaya-Krull) lemmas. They concern finitely-generated A-modules.

We say M is *finitely generated* (abbrev. *f.g.*) if M is a quotient of the free A-module A^n for some positive integer n. Equivalently, there exist elements $m_1, \ldots, m_n \in M$ such that every element $m \in M$ can be expressed in the form $m = a_1 m_1 + \cdots + a_n m_n$, for elements $a_i \in A$. (Note the expression is always unique if and only if $A^n \cong M$, in which case we say M is finitely-generated and *free*.)

If $I \subseteq A$ is an ideal, define $IM \subseteq M$ as the set of all finite linear combinations

$$IM = \{a_1 m_1 + \cdots + a_r m_r \mid a_i \in I, m_i \in M, \forall i\}.$$

Check that IM is an A-submodule of M, which is the smallest submodule containing all the elements of form am, where $a \in I$, $m \in M$.

Proposition 1.11.1 (NAK)**.** *If M is f.g. and $I \subseteq \mathrm{rad}_{\mathfrak{m}}(A)$, then $IM = M \Rightarrow M = 0$.*

Proof. Suppose $M \neq 0$ and choose a *minimal* set of generators $m_1, \ldots, m_n$, for a positive integer n. Using $M = IM$, write $m_1 = a_1 m_1 + \cdots + a_n m_n$, for elements $a_i \in I \subset \mathrm{rad}_{\mathfrak{m}}(A)$. Observe that the element $(1 - a_1)m_1$ is contained in $Am_2 + \cdots + Am_n$, and since $1 - a_1$ is a unit in A, so is the element m_1. This means that $m_2, \ldots, m_n$ generate M, violating the minimality and giving us a contradiction of the hypothesis $M \neq 0$. □

Corollary 1.11.2. *Suppose $I \subset \mathrm{rad}_{\mathfrak{m}}(A)$. If $N \subset M$ is a submodule, and M is f.g., then $M = N + IM \Rightarrow M = N$.*

Proof. Apply Prop. 1.11.1 to M/N. □

Now we specialize to the case where A is a *local* ring. Recall that $(A, \mathfrak{m})$ is *local* if $\mathfrak{m}$ is the unique maximal ideal of A. In this case $A - \mathfrak{m} = A^\times$, i.e. the units in A are precisely the elements outside of $\mathfrak{m}$. Conversely, if A has a ideal I such that $A - I \subset A^\times$, then A, I is local. Indeed, let $\mathfrak{m}'$ be a maximal ideal that is not contained in I, and choose $x \in \mathfrak{m}' - I$. This is impossible since $x \notin I \Rightarrow x \in A^\times$. Thus I is maximal, and is the unique such.

Examples of local rings

- Any field

- The p-adic numbers $\mathbb{Z}_p$ (we'll come back to these)
- Power series rings $k[[X]]$, where k is a field (ditto).

Of course, for local rings $\mathrm{rad}_{\mathfrak{m}}(A) = \mathfrak{m}$, so the NAK lemma becomes even simpler. Here is a consequence:

Corollary 1.11.3. *Suppose M is f.g. over a local ring $(A, \mathfrak{m})$, and write $k := A/\mathfrak{m}$ for the residue field. If $\overline{x_1}, \ldots, \overline{x_n}$ generate $M/\mathfrak{m}M$ as a k-vector space, then $x_1, \ldots, x_n$ generate M as an A-module.*

Proof. Appy Cor. 1.11.2 to $N = Ax_1 + \cdots + Ax_n$ and $I = \mathfrak{m}$. □

2. Lecture 2

2.1. **Improved NAK lemma.** For a f.g. A-module M we can use the following "determinant trick" (essentially the Cayley-Hamilton theorem generalized from fields to commutative rings):

Lemma 2.1.1 (Cayley-Hamilton)**.** *Let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq IM$, for an ideal $I \subseteq A$. Then ϕ satisfies an equation of the form*

$$\phi^r + a_{r-1}\phi^{r-1} + \cdots + a_0 = 0,$$

where $a_i \in I$ for all i.

Proof. Let $x_1, \ldots, x_r$ generate M. We may write $\phi(x_i) = \sum_j a_{ij}x_j$, for elements $a_{ij} \in I$. Thus for all i

$$\sum_j (\phi\delta_{ij} - a_{ij})x_j = 0,$$

where δ_{ij} is the Kronecker delta. Multiplying the matrix $(\phi\delta_{ij} - a_{ij})$ on the left by its adjoint, we get $\det(\phi\delta_{ij} - a_{ij})$ annihilates each x_i, hence is the zero endomorphism of M. Expanding out the determinant gives the desired equation. □

Remark. We used the "Cramer's Rule" $\mathrm{adj}(X) \cdot X = \det(X)\, I_n$ for any $n \times n$ matrix X over a commutative ring A. This can be deduced from the case where A is a field. Indeed, the formula is equivalent to n^2 polynomial relations in the entries of X. It is enough to prove these relations hold in the polynomial ring $\mathbb{Z}[X_{ij}]$ in n^2 indeterminates X_{ij}, and those relations follow in turn from the relations in the rational function field $\mathbb{Q}(X_{ij})$. This kind of trick is quite common to prove statements for commutative rings which are already known to hold over fields. For instance, use it to do the following exercise.

Exercise 2.1.2. *Let A be a commutative ring. Show that for $X, Y \in M_n(A)$, $\det(XY) = \det(X)\det(Y)$. Deduce from this and Cramer's rule that X has an inverse in $M_n(A)$ if and only if $\det(X) \in A^\times$.*

Corollary 2.1.3 (Improved NAK)**.** *If M is f.g. and $IM = M$, then there exists $a \in A$ with $a \equiv 1 \bmod I$, and $aM = 0$.*

Proof. Take $\phi = \mathrm{id}$ in Lemma 2.1.1, and note that $a := 1 + a_{r-1} + \cdots + a_0$ works. □

Note that this corollary gives another proof of Prop. 1.11.1: $I \subset \mathrm{rad}_{\mathfrak{m}}(A)$ means that $a \in A^\times$, and so $aM = 0$ implies $M = 0$.

2.2. **Some applications of NAK.** Here we give two quick applications of the NAK lemmas.

1st application.

Proposition 2.2.1. *Suppose $f : M \to M$ is a surjective A-module endomorphism of a f.g. A-module M. Then f is injective, hence is an automorphism.*

Proof. Using f we define on M the structure of an $A[X]$-module by setting $X \cdot m = f(m)$. By Improved NAK applied to $A[X]$ and $I = (X)$ there exists $Y \in A[X]$, such that $(1 + YX)M = 0$. Now let $u \in \ker(f)$. We have $0 = (1 + YX)(u) = u + Yf(u) = u$. Hence $\ker(f) = 0$, as desired. □

The following related result is actually proved using a different argument. (If you are not already familiar with Noetherian rings, we will return to these again later.)

Exercise 2.2.2. *Suppose A is a Noetherian ring. Then any surjective ring homomorphism $f : A \to A$ is injective, hence an automorphism.*

The following exercise can be proved using the proposition.

Exercise 2.2.3. *Let A be a commutative ring, and suppose that as A-modules, $A^n \cong A^m$. Prove that $n = m$.*

2nd application.

Recall that an A-module P is *projective* if it has the following property: let $f : M \to N$ be a surjective morphism, and let $\phi : P \to N$ be any morphism; then there exists a morphism $\psi : P \to M$ such that $f \circ \psi = \phi$. In other words, the natural map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ induced by f is *surjective*.

It is easy to prove that *P free $\Rightarrow$ P projective*. Also, it is easy to show the following result.

Proposition 2.2.4. *P is projective if and only if it is a direct summand of a free module.*

If you haven't seen these statements before, you should try to prove them yourself, but you can also look them up in N. Jacobson's book, *Basic Algebra II* (or in pretty much any book on basic algebra).

We have the following sharper result when $(A, \mathfrak{m})$ is local, our second application of the NAK lemma.

Proposition 2.2.5. *Let M be a f.g. projective module over a local ring $(A, \mathfrak{m})$. Then M is free.*

Proof. This result actually holds without the assumption "f.g." – see [Mat2], Thm. 2.5. We shall not need it in that generality.

Choose a minimal generating set $m_1, \ldots, m_n$ for M, and define the surjective map $\phi : F = A^n \to M$ by $(a_1, \ldots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n$. Let $K := \ker(\phi)$. The minimal basis property shows that

$$\sum_i a_i m_i = 0 \Rightarrow a_i \in \mathfrak{m}, \forall i.$$

Thus $K \subseteq \mathfrak{m}F$. Because M is projective, there exists $\psi : M \to F$ such that $F = K \oplus \psi(M)$, and it follows that $K = \mathfrak{m}K$. Since K is a quotient of F, it is also f.g. over A, hence by NAK, $K = 0$. This shows $F \cong M$, so M is free. □

2.3. **Special kinds of rings.** A *Euclidean domain* is a ring where a division algorithm holds (I am not going to make this precise). Examples are $\mathbb{Z}$, and $k[X]$, where k is any field.

A *PID* is a domain wherein every ideal is principal, i.e., generated by a single element.

A *UFD* is a ring wherein every non-zero, non-unit element can be written as a unit times a product of irreducible elements, in an essentially unique way. Again, I am not going to make this precise.

The following implications hold: Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD. Further, if A is a UFD, then $A[X]$ is also (Gauss' lemma); but $A[X]$ need not be Euclidean (resp. PID) even if A is. Can you give some examples showing what goes wrong?

2.4. **Classifying the prime/max ideals in ring.** Consider the ring $\mathbb{C}[X]$. This is a Euclidean domain, hence as above it is a PID hence a UFD. Hence, $\mathbb{C}[X_1, \ldots, X_n]$ is also a UFD for any $n \geq 1$. This gives rise to some natural questions:

- What are the prime/maximal ideals in $\mathbb{C}[X_1, \ldots, X_n]$?
- What are the irreducible elements in the UFD $\mathbb{C}[X_1, \ldots, X_n]$?

Consider again the case $\mathbb{C}[X]$. The non-zero prime ideals are generated by the irreducible polynomials. By the fundamental theorem of algebra, these are precisely those of the form $X - \alpha$, where $\alpha \in \mathbb{C}$. Therefore, as a *set*, we have an identification

$$\mathrm{Spec}_{\mathfrak{m}}\mathbb{C}[X] = \mathbb{C}.$$

To fully understand what we can say about $\mathbb{C}[X_1, \ldots, X_n]$, we need algebraic geometry.

2.5. **Maximal ideals in $\mathbb{C}[X_1, \ldots, X_n]$ – first step.** Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$. Evaluation at this point, i.e. the map $f \mapsto f(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}$, gives us a surjective homomorphism

$$\mathrm{ev}_{\underline{\alpha}} : \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}.$$

The kernel is a maximal ideal, call it $\mathfrak{m}_{\underline{\alpha}}$.
Claim: $\mathfrak{m}_{\underline{\alpha}} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.
Proof. The inclusion $\supseteq$ is clear. If $f \in \mathfrak{m}_{\underline{\alpha}}$, then write it as a polynomial in $X_n - \alpha_n$, with coefficients in $\mathbb{C}[X_1, \ldots, X_{n-1}]$. The constant (i.e. $\deg_{X_n} = 0$) term is a polynomial in $X_1, \ldots, X_{n-1}$ vanishing at $(\alpha_1, \ldots, \alpha_{n-1})$. By induction, that constant term is in $(X_1 - \alpha_1, \ldots, X_{n-1} - \alpha_{n-1})$, so we're done. □

Deeper fact we'll soon show (from **Hilbert's Nullstellensatz**): All maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$ are of the form $\mathfrak{m}_{\underline{\alpha}}$. Hence, like for $\mathbb{C}[X]$, we will have an identification

$$\mathrm{Spec}_{\mathfrak{m}}\mathbb{C}[X_1, \ldots, X_n] = \mathbb{C}^n.$$

2.6. **Zariski topology.** Let A be a ring. We are going to put a topology on the set $\mathrm{Spec}A$ (we'll put the subspace topology on the subset $\mathrm{Spec}_{\mathfrak{m}}A$). From the above remarks, this will actually define a new and interesting topology on the familiar set $\mathbb{C}^n$, which is very different from the "standard" metric topology.

3. Lecture 3

3.1. **Definition of Zariski topology.** Recall that to define a topology on a set X is to specify a collection $\mathfrak{U}$ of subsets of X (called "open") satisfying the following axioms:
- $\emptyset, X \in \mathfrak{U}$
- Let I be any index set. If for all $i \in I$, $U_i \in \mathfrak{U}$, then $\cup_{i\in I} U_i \in \mathfrak{U}$
- If $U, V \in \mathfrak{U}$, then $U \cap V \in \mathfrak{U}$.

To determine the topology, it is enough to specify the "closed" sets, which by definition are the complements of the open sets. (I leave it to you to formulate the axioms the closed sets must verify – see below.) That is how we will define the topology on $\mathrm{Spec}(A)$.

Namely, for any subset $E \subset A$, define

$$V(E) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supset E\}.$$

Now we show that the subsets $V(E) \subset \mathrm{Spec}(A)$ are the closed sets in a topology, which we call the **Zariski topology** on $\mathrm{Spec}(A)$. Parts (ii)-(iv) of the following lemma accomplish this. The other parts are also useful.

Lemma 3.1.1. *The following properties hold.*

(i) $V(E) = V(\langle E\rangle)$, *where* $\langle E\rangle$ *is the ideal generated by* E.
(ii) $V(\emptyset) = V(0) = \mathrm{Spec}(A)$, *and* $V(1) = \emptyset$.
(iii) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$, *where* IJ *is the ideal generated by the set of products* xy *with* $x \in I$ *and* $y \in J$.
(iv) *Let* I *be any index set. Then* $\cap_{i\in I} V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i) = V(\cup_i \mathfrak{a}_i)$.
(v) $I \subset J \implies V(J) \subset V(I)$.
(vi) $V(I) = V(r(I))$.
(vii) $V(I) \subset V(J) \Longleftrightarrow r(J) \subset r(I)$.

Note that (ii)-(iv) show we get a topology, whereas (i) and (v)-(vii) show that $I \mapsto V(I)$ *gives an order-reversing bijective correspondence*

$$\{\textit{radical ideals in } A\} \longleftrightarrow \{\textit{closed subsets in } \mathrm{Spec}(A)\}.$$

Proof. Parts (i),(ii), and (v) are clear. Parts (vi) and (vii) follow using (1.8.1).

Part (iv) is also easy from the definitions.

Let us prove (iii). The inclusions $V(I)\cup V(J) \subseteq V(I\cap J) \subseteq V(IJ)$ are easy: use (v) applied to the inclusions $I \cap J \subseteq I$ (resp. $I \cap J \subseteq J$) and $IJ \subseteq I \cap J$. Now to prove $V(IJ) \subseteq V(I) \cup V(J)$, assume $\mathfrak{p} \in V(IJ)$, i.e., $\mathfrak{p} \supset IJ$. If $\mathfrak{p} \not\supseteq I$ and $\mathfrak{p} \not\supseteq J$, then there exist $x \in I - \mathfrak{p}$ and $y \in J - \mathfrak{p}$; but note that $xy \in IJ \subset \mathfrak{p}$. This is nonsense since $\mathfrak{p}$ is prime. □

3.2. **Some further remarks about the Zariski topology.** The following remarks help us get a grip on the strange properties of the Zariski topology.

- If $\mathfrak{p}$ is a prime ideal, it is also a *point* in the topological space $\mathrm{Spec}(A)$. When we think of it as a point, we often write it as $\mathfrak{p}_x$ (the symbol x is often used to denote a point in a space, thus the subscript reminds us to think of the ideal as a point in the space). With this notation, the following equation describes the closure of the point $\mathfrak{p}_x$:

$$\overline{\{\mathfrak{p}_x\}} = V(\mathfrak{p}_x). \tag{3.2.1}$$

Let us prove this. The closure is the intersection of all closed sets containing $\mathfrak{p}_x$, that is, the closure is

$$\bigcap_{I \subseteq \mathfrak{p}} V(I) = V(\sum_{I \subseteq \mathfrak{p}} I) = V(\mathfrak{p}).$$

This is striking: a point in our space $\mathrm{Spec}(A)$ is *not* usually a *closed set*! In fact, it follows that

(3.2.2) $\mathfrak{p}_x$ is a closed point if and only if $\mathfrak{p}_x$ is a maximal ideal.

• The space $\mathrm{Spec}(A)$ is not Hausdorff, but is T_0: for any two distinct points x, y, there exists an open U containing x but not y, or vice-versa. (Prove this!)

• If A is a domain, then $\mathrm{Spec}(A) = \overline{\{0\}}$ (and the ideal (0) is called the "generic point" : it is a single point, but it is actually dense in the whole space!).

• $\mathrm{Spec}(A)$ is *compact*: any cover by open subsets has a finite sub-covering.

Proof. Suppose $\mathrm{Spec}(A) = \bigcup_{i \in I} U_i$, where U_i is the open complement of a closed set, call it $V(\mathfrak{a}_i)$. Taking complements, we find

$$\begin{aligned} &\bigcap_i V(\mathfrak{a}_i) = \emptyset = V(1) \\ &\implies V(\sum_i \mathfrak{a}_i) = V(1) \\ &\implies r(\sum_i \mathfrak{a}_i) = (1) \\ &\implies 1 \in \sum_i \mathfrak{a}_i. \end{aligned}$$

Thus, on renumbering, we may assume $1 \in \sum_{i=1}^{r} \mathfrak{a}_i$, which in turn entails

$$\cap_{i=1}^{r} V(\mathfrak{a}_i) = \emptyset,$$

i.e. $U_1, \ldots, U_r$ cover $\mathrm{Spec}(A)$. □

Exercise 3.2.1. *At this point, it is instructive to work through exercises 15-21, Chapter 1, of the book by Atiyah-Macdonald.*

3.3. **Integral extensions.** Recall that our immediate goal is to classify all the maximal ideals in a polynomial ring such as $\mathbb{C}[X_1, \cdots X_n]$. We will do this using **Hilbert's Nullstellensatz**. Our approach to that theorem is to first prove **Noether's Normalization Theorem**. That requires us to first explain the basic facts about integral extensions of rings.

Suppose $A \subset B$ is a subring. We say $b \in B$ is *integral over* A if b satisfies a monic polynomial of the form $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$, with $a_i \in A$ for all $i = 0, \ldots, n-1$.

Proposition 3.3.1. *The following properties are equivalent.*

(a) *$b \in B$ is integral over A;*
(b) *$b \in C \subset B$, for some subring C containing A, which is finitely generated as an A-module.*

Proof. $(a) \implies (b)$: Take $C = A[b]$, the subring generated by A and b. By induction on r (the case $r = 0$ following from (a)), check that $b^{n+r} \in A + Ab + \cdots + Ab^{n-1}$, for all $r \geq 0$. This proves that $C = A[b] = A + Ab + \cdots + Ab^{n-1}$, hence is f.g. as an A-module.

$(b) \implies (a)$: Apply Lemma 2.1.1 with $M = C$, $I = A$, and $\phi =$ multiplication by b. □

For a subring $A \subset B$, define $\widetilde{A} := \{b \in B \mid b \text{ is integral over } A\}$. This set $\widetilde{A}$ is called the *integral closure of A in B*.

Corollary 3.3.2. *$\widetilde{A}$ is a subring of B.*

Proof. Let $x, y \in \widetilde{A}$. We need to show $xy, x \pm y \in \widetilde{A}$. Let $A[x, y]$ be the subring of B generated by A and the elements x, y. Using Proposition 3.3.1 we see that $A[x]$ is f.g. as an A-module, and $A[x, y]$ is f.g. as an $A[x]$-module. Then the subring $A[x, y]$ is f.g. as an A-module. Since $A[x, y]$ contains xy and $x \pm y$, Proposition 3.3.1 implies that these elements are integral over A, and we're done. □

Remark: Note that a similar argument shows: if the elements $x_1, \ldots, x_n \in B$ are integral over A, then the ring $A[x_1, \ldots, x_n]$ is f.g. as an A-module.

Exercise 3.3.3. *Consider the complex numbers $\alpha = e^{2\pi i/3}$ and $\beta = e^{2\pi i/4}$. These are both integral over $\mathbb{Z}$. Find the minimal polynomial for $\alpha + \beta$, i.e., the minimal-degree monic polynomial $F(X)$ with $\mathbb{Z}$-coefficients such that $F(\alpha + \beta) = 0$.*

Corollary 3.3.4. *Consider ring inclusions $A \subset B \subset C$. If C is integral over B and B is integral over A, then C is integral over A.*

Proof. Let $c \in C$, and suppose it satisfies a polynomial relation of form $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$. Then $A[b_0, \ldots, b_{n-1}, c]$ is a f.g. A-module (check this – you will need to invoke the remark above). Thus c is integral over A by Proposition 3.3.1. □

In particular, we see that $\widetilde{\widetilde{A}} = \widetilde{A}$.

We shall prove much more about integral extensions later. But to finish our preparations for **Noether Normalization**, we content ourselves with just one more thing.

Lemma 3.3.5. *Suppose $A \subset B$ are domains, with B integral over A. Then A is a field if and only if B is a field.*

Proof. ($\Rightarrow$): Assume $b \neq 0$ and suppose $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ is a *minimal degree* monic polynomial satisfied by b. Then $a_0 \neq 0$, so $a_0^{-1} \in A$. But then

$$b^{-1} = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in B,$$

which shows that B is a field.
($\Leftarrow$): Assume $a \neq 0$. Then $a^{-1} \in B$ implies that there exists a relation, with all $\alpha_i \in A$, of form

$$a^{-n} + \alpha_{n-1}a^{-n+1} + \cdots + \alpha_0 = 0.$$

Multiplying this by a^{n-1}, we deduce that $a^{-1} \in A$, and so A is a field. □

3.4. **Aside: Beginning facts about integrally closed domains.** We now pause a moment to briefly discuss integrally closed domains. Assume A is a *domain*, with field of fractions K. In this case $\widetilde{A} \subset K$ is called simply the integral closure of A (in its fraction field). We say A is *integrally closed* (or *normal*) if $\widetilde{A} = A$. The following lemma provides lots of examples of integrally closed domains.

Lemma 3.4.1. *Any UFD is integrally closed.*

Proof. Any element in $K^\times$ may be written in the form $\frac{a}{b}$ for elements $a, b \in A - 0$. By cancelling common irreducible factors, we may assume that a and b have no factors in common.

Now the integrality condition yields, for some elements $\alpha_i \in A$, the equation

$$(\frac{a}{b})^n + \alpha_{n-1}(\frac{a}{b})^{n-1} + \cdots + \alpha_0 = 0,$$

which implies after clearing denominators

$$a^n + \alpha_{n-1}a^{n-1}b + \cdots + \alpha_0 b^n = 0.$$

But then any irreducible factor dividing b also divides a^n and hence also a, a contradiction. So b is a unit and $\frac{a}{b} \in A$. □

Question 1: Do there exist integrally closed domains which are not UFD's? The answer is YES; we shall show later that if A is a Noetherian domain, then A is a UFD if and only if it is integrally closed, and every fractional ideal is principal. We'll come back to this, but for the moment let me highlight one consequence: for Dedekind domains (which are automatically integrally closed), we have UFD $\iff$ every fractional ideal is principal $\iff$ PID. This is important in number theory.
Question 2: When is a domain integrally closed? We will give one complete answer to this question in this course (but there are other, more useful answers). Here is an interesting result we will prove later. Assume k is a field, and $\mathrm{char}(k) \neq 2$. Let $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$, and suppose f is not a square. Then

$$k[X_1, \ldots, X_n, Z]/(Z^2 - f) \text{ is integrally closed} \iff f \text{ is square-free.}$$

Recall that f is square-free means that it is not divisible by the square of any irreducible element.

3.5. **Algebraic independence.** Let k be any field, and let R be a k-algebra. By definition, this means that R is a ring containing k. More generally we can define the notion of an *A-algebra* for any commutative ring A. This is just a ring B together with a ring homomorphism $f : A \to B$. Then we may define on B the structure of an A-module by setting $a \cdot b := f(a)b$, where the multiplication on the right is that in B. The A-module structure on B is compatible with the ring structure on B in an obvious sense (formulate it!).

Return now to $k \subset R$. We say elements $u_1, \ldots, u_n \in R$ are *algebraically independent over k* if there is no non-zero polynomial $F(U_1, \ldots, U_n)$ in the polynomial ring $k[U_1, \ldots, U_n]$ such that $F(u_1, \ldots, u_n) = 0$. In that case, the map $U_i \mapsto u_i$ induces an isomorphism of rings $k[U_1, \ldots U_r] \cong k[u_1, \ldots, u_n]$.

3.6. **Noether Normalization.** From now on, we will often use the following terminology: Suppose B is an A-algebra. We say B is *module finite*, or simply *finite* over A if B is finite-generated as an A-module. We say B is a f.g. A-algebra if B can be written as a quotient ring of $A[Y_1, \ldots, Y_r]$, for some finite number of variables $Y_1, \ldots, Y_r$. In that case, we often write $B = A[y_1, \ldots, y_r]$, where here the y_i are the images of the Y_i under the quotient map.

Theorem 3.6.1 (Noether Normalization)**.** *Let k be a field, and suppose R is a f.g. k-algebra, $R = k[u_1, \ldots, u_n]$. Then there exist algebraically independent elements $x_1, \ldots, x_t$ (with $t \leq n$), such that R is module finite over $k[x_1, \ldots, x_t]$.*

Moreover, $t < n$ unless $u_1, \ldots, u_n$ are algebraically independent.

I learned the following proof from Mel Hochster many years ago.

Proof. We use induction on n. If $n = 0$, there is nothing to prove. Suppose $n \geq 1$ and assume the result is true for algebras generated by $n-1$ elements. If $u_1, \ldots, u_n$ are algebraically independent, there is nothing to prove. So WLOG [1] there exists $F \neq 0$ with $F(u_1, \ldots, u_n) = 0$. WLOG, U_n occurs in F.

Choose a positive integer N with $N > \deg(F)$.

We have $R = k[v_1, \ldots, v_n]$, where by definition $v_i := u_i - u_n^{N^i}$ for $1 \leq i \leq n-1$, and $v_n := u_n$. Define new indeterminates $V_1, \ldots, V_n$, and define $G \in k[V_1, \ldots, V_n]$ by

$$G(V_1, \ldots, V_n) = F(V_1 + V_n^N, \ldots, V_{n-1} + V_n^{N^{n-1}}, V_n).$$

Note that $G(v_1, \ldots, v_n) = 0$.

Claim: $G =$ (non-zero scalar) $\cdot$ (monic in V_n with coefficients in $k[V_1, \ldots, V_{n-1}]$).

Once we establish the claim, we will know that R is module finite over $k[v_1, \ldots, v_{n-1}]$, which by induction is module finite over $k[x_1, \ldots, x_t]$, where $t \leq n-1$. Thus we will be done.

Proof of Claim: Letting ν stand for the n-tuple of non-negative integers $(\nu_1, \ldots, \nu_n)$, we write

$$F = \sum_{\nu} \lambda_\nu U_1^{\nu_1} \cdots U_n^{\nu_n}.$$

Here we let ν range over the n-tuples with $\lambda_\nu \neq 0$. Thus

$$\begin{aligned} G &= \sum_{\nu} \lambda_\nu (V_1 + V_n^N)^{\nu_1} \cdots (V_{n-1} + V_n^{N^{n-1}})^{\nu_{n-1}} V_n^{\nu_n} \\ &= \sum_{\nu} \lambda_\nu [V_n^{\delta(\nu)} + \text{lower terms in } V_n \text{ with coeff's in } k[V_1, \ldots, V_{n-1}]], \end{aligned}$$

where $\delta(\nu) := \nu_n + \nu_1 N + \nu_2 N^2 + \cdots + \nu_{n-1} N^{n-1}$.

Choose now a ν' such that $\delta(\nu')$ is *maximal*. Then the highest $\deg_{V_n}$ term that appears anywhere is

$$\lambda_{\nu'} V_n^{\delta(\nu')}.$$

This term can't be cancelled; in fact there is *only one* ν' which maximizes the function δ. Why? Because of the uniqueness of base N expansions! This completes the proof of the claim. □

[1] Without Loss Of Generality.

3.7. **Aside: Geometric meaning of Noether Normalization.** For those of you who already know some algebraic geometry, the following is the geometric reformulation of Theorem 3.6.1.

At this point we can give *preliminary* definitions of affine variety and affine scheme. Let A be any ring. Then we will call the topological space $\mathrm{Spec}(A)$ an *affine algebraic scheme*. Now let R be a f.g. k-algebra. Then we will call the topological space $\mathrm{Spec}_{\mathfrak{m}}(R)$ an *affine algebraic variety over* k. In both cases, the complete definition of scheme/variety will be the topological space endowed with some extra structure, namely a sheaf of rings on it (stay tuned for more...).

Theorem 3.7.1. *Let $X = \mathrm{Spec}_{\mathfrak{m}}(R)$ be an affine variety over a field k. Let $\mathbb{A}^t_k$ denote t-dimensional affine space, i.e. $\mathbb{A}^t_k := \mathrm{Spec}(k[X_1, \ldots, X_t])$. Then there is a finite surjective morphism of algebraic varieties*

$$X \to \mathbb{A}^t_k$$

where $t = \dim_k(X)$.

The theorem states that every affine algebraic variety is "almost" an affine space k^t.

We will define algebraic varieties and all the necessary concepts we need to understand these statements later.

3.8. **Hilbert Nullstellensatz.** Now we apply this to get

Corollary 3.8.1 (Nullstellensatz - weak form)**.** (1) *Let R be a f.g. k-algebra. Assume R is a field. Then R is a finite field extension of k.*
(2) *If $k = \overline{k}$ (i.e. k is algebraically closed), then moreover $R = k$.*

Proof. For part (1), Theorem 3.6.1 says that R is module finite over a domain of the form $k[x_1, \ldots, x_t]$. The latter must be a field, by Lemma 3.3.5. But then $t = 0$ (why?), and thus R is module finite over the field k, as desired.

For part (2), note that $k = \overline{k}$ implies that there are no non-trivial finite extensions of k, so that $R = k$ is forced. □

3.9. **Maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$ - final step.** The field $\mathbb{C}$ is algebraically closed, so we may apply the above corollary to prove that every maximal ideal is of the form $\mathfrak{m}_{\underline{\alpha}}$, for some $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$. Let $\mathfrak{m}$ be a maximal ideal, and let $R := \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{m}$. Then by the above Corollary 3.8.1, we know that the inclusion $\mathbb{C} \hookrightarrow R$ is actually an isomorphism. Define α_i to the be complex number which is the image of X_i under the homomorphism

$$\mathbb{C}[X_1, \ldots, X_n] \to R \cong \mathbb{C}.$$

The above map can be identified with the evaluation map $\mathrm{ev}_{\underline{\alpha}}$, and thus $\mathfrak{m} = \mathfrak{m}_{\underline{\alpha}}$.

3.10. **Further consequences of the Nullstellensatz.**

Corollary 3.10.1. *Let $\phi : R \to S$ be a homomorphism of f.g. k-algebras. Let $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(S)$. Then $\mathfrak{m}^c = \phi^{-1}(\mathfrak{m}) \in \mathrm{Spec}_{\mathfrak{m}}(R)$.*

In particular, the map $\phi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ given by $\mathfrak{p} \mapsto \mathfrak{p}^c$, takes $\mathrm{Spec}_{\mathfrak{m}}(S)$ into $\mathrm{Spec}_{\mathfrak{m}}(R)$.

Proof. The map ϕ induces an inclusion $R/\mathfrak{m}^c \hookrightarrow S/\mathfrak{m}$ of k-algebras. Since $S/\mathfrak{m}$ is a field, the Nullstellensatz implies it is a finite extension of k, and thus it is necessarily module finite over $R/\mathfrak{m}^c$. But then this latter domain is itself a field, by Lemma 3.3.5, and thus $\mathfrak{m}^c$ is maximal. □

Exercise 3.10.2. *Show that the map ϕ^* is* continuous *(see Atiyah-Macdonald, Chapter 1, #21 (i)).*

Question: If $k = \overline{k}$, we can now identify

$$\mathrm{Spec}_{\mathfrak{m}}(k[X_1, \ldots, X_n]) = k^n.$$

The Zariski topology on the left hand side thus gives us a new topology on k^n. What does this topology look like? That is the subject we will look at next.

4. Lecture 4

4.1. **Algebraic Zeros Theorem.** Let k be a field, $\overline{k}$ an algebraic closure of k. Let $\Phi \subset k[X_1, \ldots, X_n]$ be a subset. We call $\alpha = (\alpha_1, \ldots, \alpha_n) \in \overline{k}^n$ an *algebraic zero* of Φ if $f(\alpha) = 0$ for all $f \in \Phi$.

Theorem 4.1.1 (Algebraic zeros theorem)**.** *Write $k[X_1, \ldots, X_n] = k[X]$ for short.*

(i) *If Φ has no algebraic zeros, then $\langle \Phi \rangle = (1) = k[X]$.*
(ii) *If $f \in k[X]$ vanishes at every algebraic zero of Φ, then $f \in r(\langle \Phi \rangle)$.*

Proof. (i). Write $I := \langle \Phi \rangle$. If $1 \notin I$, then $I \subset \mathfrak{m}$, for a maximal ideal $\mathfrak{m}$. Since $k[X]/\mathfrak{m}$ is a finite extension of k (Corollary 3.8.1), there is an embedding of fields

$$\frac{k[X]}{\mathfrak{m}} \hookrightarrow \overline{k}.$$

Let $\alpha_i :=$ image of X_i. But then all elements of $\mathfrak{m}$ hence also I vanish at α, a contradiction. Thus, $I = (1)$.
(ii). Inside $k[X, Y]$ consider $\Phi \cup \{1 - Yf(X)\}$. This set has no algebraic zeros (why?). So by part (i) there exist functions $Q(X, Y), g_i(X, Y) \in k[X, Y]$ and $h_i(X) \in \Phi$ for $i = 1, \ldots, r$ such that

$$\sum_{i=1}^{r} g_i(X, Y)h_i(X) + Q(X, Y)(1 - Yf(X)) = 1.$$

Specializing $Y = f(X)^{-1}$, we get

$$\sum_i g_i(X, f(X)^{-1})h_i(X) = 1.$$

Now we multiply by some high power $f^N(X)$ to clear the denominators to find that

$$f^N \in \sum_i h_i k[X] \subset \langle \Phi \rangle,$$

as desired. □

Remark. Note that (i) says: if $f \in k[X_1, \ldots, X_n]$ is *not* a unit, then it has at least one zero $\alpha \in \overline{k}^n$. You already knew this for $n = 1$: any polynomial in $k[X]$ which is not a unit, has a zero in the field $\overline{k}$.

4.2. **Consequences of Nullstellensatz and Algebraic Zeros Theorem.** *1st application.*

Proposition 4.2.1. *Let R be a finitely generated k-algebra, and $I \subset R$ an ideal. Then*

$$r(I) = \bigcap_{max\ \mathfrak{m} \supseteq I} \mathfrak{m}.$$

In particular,

(1) *For any prime ideal $\mathfrak{p}$, we have $\mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$.*
(2) $\mathrm{rad}(R) = \mathrm{rad}_{\mathfrak{m}}(R)$.

Proof. Write $R = k[u_1, \ldots, u_n]$; there is a surjection

$$\phi : k[X_1, \ldots, X_n] \to R$$

given by sending $X_i \mapsto u_i$ for all i. By the correspondence of ideals between I and R with those between $J := I^c$ and $k[X, \ldots, X_n]$ (under which prime/max ideals correspond to prime/max ideals), it is enough to prove the proposition for $R = k[X_1, \ldots, X_n]$. But this case will follow from Theorem 4.1.1, (ii). We start by verifying the following: if

$$f \in \bigcap_{\max\ \mathfrak{m} \supset J} \mathfrak{m},$$

then f vanishes at every algebraic zero of J. Let's check this statement. If α is an algebraic zero of J, then J is in the kernel of

$$\mathrm{ev}_\alpha : k[X_1, \ldots, X_n] \to \overline{k}$$

and this kernel is itself a maximal ideal $\mathfrak{m}$, since the image of ev_α is a domain which is an integral extension of k (being contained in $\overline{k}$) hence by Lemma 3.3.5 is a field. Since $f \in \mathfrak{m}$, we see that f vanishes at α, as desired. Thus by (ii) of Theorem 4.1.1, we see $f \in r(J)$. □

The conclusion of Proposition 4.2.1 is not true in general for all commutative rings.

Exercise 4.2.2. (1) *Find a domain A and a proper ideal $I \subset A$ such that*

$$r(I) \subsetneq \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}.$$

(2) *Consider a* local *k-algebra $(A, \mathfrak{m})$. If A is finitely generated as a k-algebra, what can you say about the prime ideals of A?*
(3) *Suppose $(A, \mathfrak{m})$ is a local k-algebra. Show that the following are equivalent:*
   (i) *A is a f.g. k-algebra;*
   (ii) *A is an Artin ring and $A/\mathfrak{m}$ is a finite extension of k;*
   (iii) *A is Artin and each $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is finite-dimensional as a k-vector space;*
   (iv) *A is finite dimensional as a k-vector space.*
   Hint: You might want to make use of the material from Chapter 8 of Atiyah-Macdonald.

2nd application.

Proposition 4.2.3. *Let R be a f.g. k-algebra. Then* $\mathrm{Spec}_{\mathfrak{m}}(R) \subset \mathrm{Spec}(R)$ *is* dense.

Proof. There is a basis of open subsets of $\mathrm{Spec}(R)$ given by the subsets

$$D(f) := \{\mathfrak{q} \mid f \notin \mathfrak{q}\}.$$

[Aside: to check $\{D(f)\}_{f\in R}$ indeed form a basis for a topology, we need to check that if $\mathfrak{q} \in \mathrm{Spec}(R) - V(I)$, then there exists a $D(f)$ with $\mathfrak{q} \in D(f) \subset \mathrm{Spec}(R) - V(I)$. But just take f to be any element in $I - \mathfrak{q}$.]

We will show: if $\mathfrak{p} \in D(f)$, then there exists a maximal ideal $\mathfrak{m}$ with

- $\mathfrak{m} \supset \mathfrak{p}$;
- $\mathfrak{m} \in D(f)$.

But this is obvious from Prop. 4.2.1, (1). Clearly this also shows $\mathrm{Spec}_{\mathfrak{m}}(R)$ is dense in $\mathrm{Spec}(R)$. □

Exercise 4.2.4. *Find a ring A such that $\mathrm{Spec}_{\mathfrak{m}}(A)$ is* not *dense in $\mathrm{Spec}(A)$.*

4.3. **Closed subsets in $\overline{k}^n$ and radical ideals.** In this subsection we assume $k = \overline{k}$, and let $R = k[X_1, \ldots, X_n]$.

We have established an identification of sets $\mathrm{Spec}_{\mathfrak{m}}(R) = k^n$ (the same proof we gave for $k = \mathbb{C}$ works, as we only used the property that $\mathbb{C}$ is algebraically closed). The left hand side is given the Zariski topology: more precisely, the subspace topology it inherits from the Zariski topology on $\mathrm{Spec}(R)$. What does this mean concretely? First we note that under the identification $\mathrm{Spec}_{\mathfrak{m}}(R) = k^n$, we have:

$$\begin{aligned} Z \subset k^n \text{is closed} &\iff Z = \mathrm{Spec}_{\mathfrak{m}}(R) \cap V(I), \text{for some (radical) ideal } I \subset R \\ &\iff Z = \{\alpha \in k^n \mid f(\alpha) = 0, \forall f \in I\} =: Z(I). \end{aligned}$$

This leads us to define

- For a subset $Y \subset k^n$, let $\mathcal{I}(Y) := \{f \in R \mid f(y) = 0, \forall y \in Y\}$;
- For an ideal $I \subset R$, let $Z(I) := \{\alpha \in k^n \mid f(\alpha) = 0, \forall f \in I\}$.

Note that $\mathcal{I}(Y)$ is always a *radical* ideal, and $Z(I)$ is always a *closed* subset.

Theorem 4.3.1 (Classical Nullstellensatz – 1st form)**.** *Let $I \subset R$ be any ideal, and let $Y \subset k^n$ be any subset, with Zariski-closure $\overline{Y}$. Then we have:*

(a) $\mathcal{I}(Z(I)) = r(I)$.
(b) $Z(\mathcal{I}(Y)) = \overline{Y}$.

In particular, $I \mapsto Z(I)$ gives an order-reversing bijection

$$\{\textit{radical ideals in } R\} \longleftrightarrow \{\textit{Zariski closed subsets in } k^n\},$$

with inverse $Z \mapsto \mathcal{I}(Z)$.

Proof. (a): The Algebraic zeros theorem (ii) gives the non-trival inclusion $\subseteq$.
(b): Clearly $Z(\mathcal{I}(Y)) \supseteq Y$, hence $Z(\mathcal{I}(Y)) \supseteq \overline{Y}$.

By the Lemma below, it is enough to show that equality holds *after we apply* $\mathcal{I}(\cdot)$. But then the equality we want can be derived using part (a) (using that $\mathcal{I}(Y)$ is radical):

$$\mathcal{I}Z(\mathcal{I}(Y)) = \mathcal{I}(Y) = \mathcal{I}(\overline{Y}).$$

Here, the last equality holds because polynomial functions are *continuous* as functions $k^n \to k$ (check this!–see Exercise below). □

Lemma 4.3.2. *Suppose for Zariski closed subsets $Y_1 \supseteq Y_2$ we have $\mathcal{I}(Y_1) = \mathcal{I}(Y_2)$. Then $Y_1 = Y_2$.*

Proof. Suppose not. Then there is a point $\alpha \in Y_1 - Y_2$. There is a principal open subset $D(f) = \{x \in k^n \mid f(x) \neq 0\}$, such that $\alpha \in D(f)$, but $D(f) \cap Y_2 = \emptyset$. Then we see that f vanishes on Y_2, i.e. $f \in \mathcal{I}(Y_2)$. Since the latter ideal is also $\mathcal{I}(Y_1)$ by hypothesis, we see that f also vanishes on Y_1, hence on α, a contradiction. □

Exercise 4.3.3. *Give k and k^n the Zariski topologies. Show that all polynomials are continuous as functions $k^n \to k$.*

4.4. **Examples.** We can draw some pictures of $Z(I)$ for various ideals $I \subset \mathbb{C}[X, Y, Z]$.
- $X^2 - Y^2 - Z = 0$: saddle point at origin.
- $X^4 + (Y^2 - X^2)Z^2 = 0$: figure-8 cones along Z-axis emanating from origin.
- $X^2 + Z^3 = 0$: tent draped over Y-axis through origin.
- $I = (XY, YZ)$, i.e., both $XY = 0$ and $YZ = 0$: union of the Y-axis and the XZ-plane.

To see this last example, note that $Z(I) = Z(XY) \cap Z(YZ)$, and $Z(XY)$ is the union of the YZ-plane and the XZ-plane. Similarly, $Z(YZ)$ is the union of the XZ-plane and the XY-plane. Hence the intersection $Z(I)$ is the union of the Y-axis and the XZ-plane.

5. Lecture 5

5.1. **Classical Nullstellensatz for reduced f.g k-algebras.** We call a ring A *reduced* provided $\mathrm{rad}(A) = 0$; in other words, A has no non-zero nilpotent elements. For example, if $J \subset k[X] = k[X_1, \ldots, X_n]$ is a radical ideal, then the quotient $R = k[X]/J$ is reduced.

Now we can give a more complete version of the classical Nulltstellensatz, this time for arbitrary *reduced* f.g. k-algebras in place of $k[X] = k[X_1, \ldots, X_n]$. Let R and J be as in the previous paragraph. Again assume $k = \overline{k}$. Let $V := Z(J) \subset k^n$, a Zariski closed subset. As before, the statement should concern radical ideals of R and Zariski-closed subsets in V.

We can extend our previous definitions of the maps $Z(\cdot)$ and $\mathcal{I}(\cdot)$ as follows. Via contraction, the ideals $I \subset R$ correspond bijectively to ideals $I^c \subset k[X]$ which contain J, and radical ideals correspond to radical ideals. Therefore, we may set $Z(I) := Z(I^c) \subset k^n$. Note that $I^c \supseteq J$ implies (by Theorem 4.3.1) that $Z(I) \subseteq Z(J) =: V$. Thus $I \subset R$ gives us a Zariski-closed subset of k^n which is contained in the Zariski-closed subset $V \subset k^n$.

In the reverse direction, any Zariski-closed subset $Y \subset V$ is also Zariski-closed as a subset of k^n, and $\mathcal{I}(Y)$ is a radical ideal of $k[X]$ which contains $\mathcal{I}(V) = J$, by Theorem 4.3.1. We can therefore regard $\mathcal{I}(Y)$ as a radical ideal of R.

The two operations $I \mapsto Z(I)$ and $Y \mapsto \mathcal{I}(Y)$ are mutually inverse (just use (a),(b) of Theorem 4.3.1 to see this). We have proved:

Theorem 5.1.1 (Classical Nullstellensatz – final form)**.** *Let $J \subset k[X]$ be a radical ideal and $R := k[X]/J$. The rule $I \mapsto Z(I)$ gives an order-reversing bijection*

$$\{\textit{radical ideals in } R\} \longleftrightarrow \{\textit{Zariski closed subsets in } V\},$$

with inverse $Z \mapsto \mathcal{I}(Z)$.

5.2. **Remarks on irreducible sets and dimension.** What is the dimension of an arbitrary topological space X? Here we give one reasonable definition that works in algebraic geometry (but not in classical geometry), using the notion of irreducible subset.

We call a a topological space X *irreducible* provided the following equivalent conditions are satisfied:

- Any two non-empty open subsets in X intersect;
- Every non-empty open subset in X is dense in X;
- X is not the union of two proper closed subsets.

Note that this concept is not very interesting for Hausdorff spaces: a non-empty Hausdorff space is irreducible if and only if it consists of a single point.

If $Y \subset X$ is a subset, we give it the subspace topology, and then we say Y is irreducible, if it is irreducible once it is given that topology.

We now define the **Krull dimension** of X to be

$$\mathrm{Krulldim}(X) = \sup\{n \in \mathbb{N} \mid \exists \text{ closed irreducible subsets } Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n\}.$$

N.B. In this definition, we require that the subsets Y_i are *non-empty* (the empty set is irreducible and we don't want to allow it in a chain).

Note that Krulldim(Haussdorff space) = 0. However, this notion of dimension works well for algebraic geometry, as we shall shortly see.

Note that any irreducible subset $Y \subset X$ is contained in a maximal irreducible subset, which is closed. Why? We need to notice two things:

(i) Zorn's lemma applied to $\Sigma = \{\text{irred. } Y' \supseteq Y\}$ shows that this collection possesses maximal elements (for a chain $\{Y'_\alpha\}$, observe that $\cup_\alpha Y'_\alpha$ is irreducible);

(ii) The closure of an irreducible set is irreducible (assume Y is irreducible; if $\overline{Y} = F_1 \cup F_2$ with F_i closed proper subsets of $\overline{Y}$, then Y is the union of the closed and proper subsets $Y \cap F_i$, violating our assumption that Y is irreducible).

Thus we may speak of the maximal irreducible subsets (which are closed) in X; we call them the **irreducible components** of X.

What are the irreducible components of $X = \mathrm{Spec}(A)$, for a ring A?

Proposition 5.2.1. *Let $A \neq 0$ be a ring.*

(i) *The non-empty closed irreducible subsets are those of the form $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal.*

(ii) *The irreducible components are the $V(\mathfrak{p})$ for $\mathfrak{p}$ a* minimal prime *ideal.*

In particular, the fact that irreducible components exist for $\mathrm{Spec}(A)$ *implies that* minimal prime ideals *exist in any ring $A \neq 0$ (compare with Atiyah-Macdonald, Ch. 1, Ex. 8).*

Proof. (i): Let I be a radical ideal. We need to show that $V(I)$ is irreducible iff I is prime. If I is not prime, then choose $x, y \notin I$ such that $xy \in I$. Let $\mathfrak{a} := I + (x) \supsetneq I$, and $\mathfrak{b} := I + (y) \supsetneq I$. Then we see that $\mathfrak{ab} \subset I$, and so $r(\mathfrak{ab}) \subset I$ and $V(I) \subset V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$. So $V(I) = (V(I) \cap V(\mathfrak{a})) \cup (V(I) \cap V(\mathfrak{b}))$, a union of *proper* closed subsets. This shows that $V(I)$ is not irreducible.

Conversely, assume $V(I) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ is a union of *proper* closed subsets, for radical ideals $\mathfrak{a}, \mathfrak{b}$. Then $\mathfrak{a} \cap \mathfrak{b}$ is still radical, and so the equality $V(I) = V(\mathfrak{a} \cap \mathfrak{b})$ shows that $I = \mathfrak{a} \cap \mathfrak{b}$. But this shows that I is not prime. Indeed, since $I \subsetneq \mathfrak{a}, \mathfrak{b}$, we have elements $x \in \mathfrak{a} - I$ and $y \in \mathfrak{b} - I$. But then $xy \in \mathfrak{a} \cap \mathfrak{b} = I$, which means I is not prime.

(ii): This follows using (i) and the fact that $V(\mathfrak{p}) \supseteq V(\mathfrak{q}) \Leftrightarrow \mathfrak{p} \subseteq \mathfrak{q}$. □

Remarks: (1) From previous work, we know that $\overline{\{\mathfrak{p}_x\}} = V(\mathfrak{p})$. This means that the point $\mathfrak{p}_x$ is *dense* in the closed irreducible set $V(\mathfrak{p})$. If $\mathfrak{p}$ is minimal, we call $\mathfrak{p}_x$ the **generic point** of the irreducible component $V(\mathfrak{p})$.

(2) In part (i) above, we actually proved the following fact (see Atiyah-Macdonald, Ch.1, Exer.19): $\mathrm{Spec}(A)$ is irreducible iff the nilradical of A is prime. Indeed, take $I = r((0))$, and note that $V(I) = \mathrm{Spec}(A)$.

The above considerations lead us to give the following definition of dimension (sometimes called Krull dimension) for a ring $A \neq 0$:

$$\dim(A) = \sup\{n \in \mathbb{N} \mid \exists \text{ prime ideals } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n\}.$$

It is not at all obvious that $\dim(A) < \infty$, and indeed sometimes $\dim(A) = \infty$, even if A is assumed to be Noetherian (Nagata's example)! However, if A is *Noetherian and local*, then it turns out that its dimension is always finite. It is also finite for certain nice rings, such as polynomial rings. Furthermore, the notion is "intuitively correct" because, as we shall see, $\dim \mathbb{C}[X_1, \ldots, X_n] = n$. One of the major parts of this course will be dimension theory of Noetherian local rings.

5.3. **Localization – definitions.** We now return to pure algebra for a while. We need to develop some technical tools to help us prove more about integral ring extensions, which will also help us work toward giving the definitions in the statement of Theorem 3.7.1.

Let $A \neq 0$ be a ring, and let $S \subset A$ be a subset. We call S a **multiplicative subset** provided $1 \in S$ and $x, y \in S \Rightarrow xy \in S$.

Given A, S, we will define a new ring $S^{-1}A$ and a homomorphism

$$A \to S^{-1}A$$

which satisfies a certain "universal property".

Let $S^{-1}A$ be the set of equivalence classes of all formal quotients $\frac{a}{s}$, for $a \in A$, $s \in S$. We say $\frac{a}{s} \sim \frac{a'}{s'}$ if and only if $\exists t \in S$ such that $t(s'a - sa') = 0$. Check that this is an equivalence relation. Sometimes we denote the equivalence classes using the symbol $[\frac{a}{s}]$.

Proposition 5.3.1. *Let $S \subset A$ be a multiplicative subset.*

1. *$S^{-1}A$ is a ring with homomorphism* $\mathrm{can} : A \to S^{-1}A$ *given by $a \mapsto [\frac{a}{1}]$.*
2. *(Universal property): If $\phi : A \to B$ is any ring homomorphism such that $\phi(S) \subset B^\times$, then there is a unique homomorphism $\tilde{\phi} : S^{-1}A \to B$ such that $\tilde{\phi} \circ \mathrm{can} = \phi$.*

The homomorphism $\tilde{\phi}$ is defined by $\tilde{\phi}[\frac{a}{s}] = \phi(a)\phi(s)^{-1}$.

Proof. This is standard and easy to prove, the main point being to show that the various ring operations and ring homomorphism are well-defined. See Atiyah-Macdonald, Ch. 3 for details. In brief, the identity element is $[\frac{1}{1}]$, and we add and multiply elements by the rules

$$[\frac{a}{s}][\frac{a'}{s'}] = [\frac{aa'}{ss'}]$$
$$[\frac{a}{s}] + [\frac{a'}{s'}] = [\frac{s'a + sa'}{ss'}].$$

□

Examples: (1) If A is a domain and $S = A - 0$, then $S^{-1}A = \mathrm{Frac}(A)$.

(2) If $\mathfrak{p}$ is prime, then $S := A - \mathfrak{p}$ is a multiplicative subset; denote $S^{-1}A$ simply by $A_{\mathfrak{p}}$.

(3) If $f \in A$, let $S := \{f^n, n \geq 0\}$. Then $S^{-1}A = A_f = A[\frac{1}{f}]$.

5.4. **Localization of modules.** The same construction works for modules: let $S \subset A$ be as above, and let M be an A-module. Then we can define in a parallel way $S^{-1}M \in S^{-1}A$-Mod. The $S^{-1}A$-module structure is defined using the rule

$$[\frac{a}{s}][\frac{m}{t}] = [\frac{am}{st}].$$

Addition is defined as in $S^{-1}A$. I leave it to you to check that the operations are well-defined, and $S^{-1}M$ really is an $S^{-1}A$-module.

The map $M \mapsto S^{-1}M$ is a functor in an obvious way (we'll discuss functors soon, so don't worry if you don't know what this means). Just note that an A-module homomorphism $f : M \to M'$ induces a well-defined $S^{-1}A$-module homomorphism $S^{-1}M \to S^{-1}M'$ given by

$$S^{-1}f([\frac{m}{s}]) = [\frac{f(m)}{s}].$$

Lemma 5.4.1. *The functor $M \mapsto S^{-1}M$ is exact, i.e. it takes exact sequences in A-Mod into exact sequences in $S^{-1}A$-Mod.*

Proof. Suppose

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact. Note that

$$\begin{aligned} \frac{m}{s} \in \ker(S^{-1}g) &\iff \exists t \in S \text{ such that } tg(m) = 0 \\ &\iff \exists t, m' \text{ such that } f(m') = tm, \text{ i.e. } f(\tfrac{m'}{st}) = \tfrac{m}{s} \\ &\iff \frac{m}{s} \in \mathrm{im}(S^{-1}f). \end{aligned}$$

□

Lemma 5.4.2. *There is an isomorphism $S^{-1}A \otimes_A M \cong S^{-1}M$ as $S^{-1}A$-modules, given by $\frac{a}{s} \otimes m \mapsto \frac{am}{s}$.*

Proof. The map is clearly surjective. We prove injectivity: every element on the LHS [2] is of form $\frac{1}{s} \otimes m$ (check this!), and $\frac{1}{s} \otimes m \mapsto 0$ implies that $\exists\ t \in S$ such that $tm = 0$, and in that case

$$\frac{1}{s} \otimes m = \frac{1}{st} \otimes tm = 0.$$

□

Recall that an A-module N is **flat** provided that the following holds:
Whenever $M' \to M \to M''$ is an exact sequence of A-modules, then the induced sequence $N \otimes_A M' \to N \otimes_A M \to N \otimes_A M''$ is also exact. In other words, the functor $N \otimes_A -$ is exact.

The following exercise provides lots of examples of flat modules.

Exercise 5.4.3. *Any free module is flat. Any projective module is a direct summand of a free module, hence is also flat.*

[2] Left Hand Side

Corollary 5.4.4. *$S^{-1}A$ is a flat A-module.*

Proof. The corollary follows from the two preceding lemmas. □

Now we can produce a lot of flat modules which are not projective (so also not free). The simplest example is $\mathbb{Q}$, a flat $\mathbb{Z}$-module which is not projective (since it's not free, and over $\mathbb{Z}$, free $\iff$ projective).

6. Lecture 6

6.1. **Further properties of localization.** In the statements below, M_i, N, P, etc. are all A-modules, and $=$ means that there is a canonical isomorphism of $S^{-1}A$-modules.

Lemma 6.1.1. *The following properties of localization hold.*

(i) $S^{-1}(M_1 \oplus M_2) = S^{-1}M_1 \oplus S^{-1}M_2$.
(ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
(iii) $S^{-1}(M/N) = S^{-1}M/S^{-1}N$.
(iv) $S^{-1}(\mathrm{rad}(A)) = \mathrm{rad}(S^{-1}A)$.
(v) $S^{-1}(M \otimes_A N) = S^{-1}M \otimes_{S^{-1}A} S^{-1}N$. *In particular, for a prime ideal $\mathfrak{p}$, we have $(M \otimes_A N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$.*

Proof. In statements (ii) and (iii), we understand N, P as submodules of a module M; by exactness of $S^{-1}(\cdot)$, we can regard $S^{-1}N, S^{-1}P$ are submodules in $S^{-1}M$. In statement (v), the isomorphism is given by

$$\frac{m \otimes n}{s} \mapsto \frac{m}{1} \otimes \frac{n}{s} = \frac{m}{s} \otimes \frac{n}{1}$$

with inverse $\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$.

The remaining statements are easy to check. □

6.2. **Local properties.** What are local properties? They are properties of an A-module M that hold iff they hold for all the localizations $M_{\mathfrak{p}}$. Why call them "local"? Because the ring $A_{\mathfrak{p}}$ turns out to be a local ring (see Prop. 6.4.1 below).

Lemma 6.2.1. *For an A-module M, the following statements are equivalent:*

(1) $M = 0$.
(2) $M_{\mathfrak{p}} = 0$ *for all* $\mathfrak{p} \in \mathrm{Spec}(A)$.
(3) $M_{\mathfrak{m}} = 0$ *for all* $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$.

Proof. (3) $\implies$ (1): For $x \in M$, define $\mathrm{Ann}(x) = \{a \in A \mid ax = 0\}$, an ideal in A. If $x \in M$ and $x \neq 0$, then $\mathrm{Ann}(x) \neq (1)$, and so $\mathrm{Ann}(x) \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. But then $\frac{x}{1} \neq 0$ in $M_{\mathfrak{m}}$, so the latter is not zero. □

Lemma 6.2.2. *For an A-module homomorphism $\phi : M \to N$, the following are equivalent:*

(1) *ϕ is injective (resp. surjective, bijective).*
(2) *$\phi_{\mathfrak{p}}$ is injective (resp. surjective, bijective) for all* $\mathfrak{p} \in \mathrm{Spec}(A)$.
(3) *$\phi_{\mathfrak{m}}$ is injective (resp. surjective, bijective) for all* $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$.

Proof. For each $\mathfrak{p}$, the following sequence is exact, by Lemma 5.4.1;

$$0 \to \ker(\phi)_{\mathfrak{p}} \to M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to \mathrm{coker}(\phi)_{\mathfrak{p}} \to 0.$$

Now use Lemma 6.2.1. □

These lemmas help us prove the following lemma ("flatness is a local property").

Lemma 6.2.3. *For an A-module M, the following are equivalent:*

(1) *M is A-flat.*
(2) *$M_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$-flat for every $\mathfrak{p} \in \mathrm{Spec}(A)$.*
(3) *$M_{\mathfrak{m}}$ is $A_{\mathfrak{m}}$-flat for every $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$.*

Proof. (1) $\implies$ (2) follows from a more general fact: Let $f : A \to B$ be a homomorphism; then M is A-flat implies that $B \otimes_A M$ is B-flat. This follows (check this!) from the fact that for any B-module N we have an isomorphism of B-modules

$$N \otimes_B (B \otimes_A M) \cong N \otimes_A M.$$

On the RHS, we are viewing N as an A-module, via the homomorphism $f : A \to B$. See Atiyah-Macdonald Ch.2 for details. The point is that we may define the A-module structure with the rule $a \cdot n := f(a)n$.

(3) $\implies$ (1): It's enough to show: if $N \hookrightarrow P$ in A-Mod, then $M \otimes_A N \hookrightarrow M \otimes_A P$ as well. But now using Lemmas 5.4.1, 6.1.1, 6.2.2, we see

$$\begin{aligned} N \hookrightarrow P &\implies N_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}}, \ \forall \mathfrak{m} \\ &\implies M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}} \hookrightarrow M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} P_{\mathfrak{m}}, \ \forall \mathfrak{m} \\ &\implies (M \otimes_A N)_{\mathfrak{m}} \hookrightarrow (M \otimes_A P)_{\mathfrak{m}}, \ \forall \mathfrak{m} \\ &\implies M \otimes_A N \hookrightarrow M \otimes_A P. \end{aligned}$$

□

6.3. **Exercises on integrality.** At this point we pause to test our understanding a little bit. The following two lemmas are exercises that I leave to you. (They can of course be found in the standard texts.)

Lemma 6.3.1. *Let A, S be as above. If $A \subset B$ is an integral extension, then so is $S^{-1}A \subset S^{-1}B$. More generally, if C is the integral closure of A in B, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

In particular, if $\mathfrak{p} \in \mathrm{Spec}(A)$ and $A \subset B$ is integral, then so is $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$.

Lemma 6.3.2. *If $A \subset B$ is an integral extension, $\mathfrak{q} \in \mathrm{Spec}(B)$ and $\mathfrak{p} := \mathfrak{q}^c \in \mathrm{Spec}(A)$, then $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is maximal.*

Exercise 6.3.3. *Prove the two lemmas above.*

Using the lemmas, we have "normality is a local property". Note that if A is a domain with fraction field K, then every localization $A_{\mathfrak{p}}$ is also a domain, with the same fraction field.

Lemma 6.3.4. *Let A be a domain with fraction field K. The following are equivalent:*

(i) *A is normal.*
(ii) *$A_{\mathfrak{p}}$ is normal for every $\mathfrak{p} \in \mathrm{Spec}(A)$.*
(iii) *$A_{\mathfrak{m}}$ is normal for every $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$.*

Proof. Consider the inclusion $f : A \hookrightarrow \widetilde{A} \subset K$, where $\widetilde{A}$ is the integral closure of A in K. Note that (i) holds iff f is surjective. Similarly, since the exercise above shows that $(\widetilde{A})_{\mathfrak{p}} = \widetilde{(A_{\mathfrak{p}})}$, (ii) (resp. (iii)) holds iff $f_{\mathfrak{p}}$ (resp. $f_{\mathfrak{m}}$) is surjective for every $\mathfrak{p}$ (resp. $\mathfrak{m}$). Now the lemma follows from Lemma 6.2.2. □

6.4. **Extending and contracting ideals along $A \to S^{-1}A$.**

Proposition 6.4.1. *Let A, S be as in the previous section.*

(1) *Every ideal in $S^{-1}A$ is an extended ideal, hence of the form $S^{-1}\mathfrak{a}$, for some ideal $\mathfrak{a} \subseteq A$.*
(2) *The rule $S^{-1}\mathfrak{p} \leftrightarrow \mathfrak{p}$ gives a bijective correspondence between the prime ideals in $S^{-1}A$ and the prime ideals in A which are disjoint from S.*

In particular, taking $S = A - \mathfrak{p}$, we see $\mathrm{Spec}(A_{\mathfrak{p}}) \leftrightarrow \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \subseteq \mathfrak{p}\}$. *Thus $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ is a local ring.*

Proof. (1): Let $\mathfrak{b} \subset S^{-1}A$ be an ideal, and suppose $\frac{x}{s} \in \mathfrak{b}$. Then $\frac{x}{1} \in \mathfrak{b}$, hence $x \in \mathfrak{b}^c$ and so $\frac{x}{s} \in \mathfrak{b}^{ce}$. But then $\mathfrak{b} \subseteq \mathfrak{b}^{ce} \subseteq \mathfrak{b}$ (the latter inclusion being automatic), hence $\mathfrak{b} = \mathfrak{b}^{ce}$.

(2): If $\mathfrak{q} \subseteq S^{-1}A$ is prime, then so is $\mathfrak{q}^c$ (and the latter clearly doesn't meet S – otherwise $\mathfrak{q}$ would contain a unit in $S^{-1}A$). Moreover that fact that $\mathfrak{q}$ is an extended ideal implies that $\mathfrak{q} = S^{-1}\mathfrak{q}^c$. (See Atiyah-Macdonald, Prop. 1.17.)

On the other hand, suppose $\mathfrak{p} \subset A$ is prime. Then $S^{-1}\mathfrak{p} \subset S^{-1}A$ is prime iff $S^{-1}A/S^{-1}\mathfrak{p} \neq 0$ and is a domain. Let $\overline{S}$ denote the image of S in $A/\mathfrak{p}$. Then $S^{-1}A/S^{-1}\mathfrak{p} \cong (\overline{S})^{-1}(A/\mathfrak{p})$. The latter ring is either zero or is a non-zero ring contained in the field of fractions of $A/\mathfrak{p}$, hence is a domain. Hence $S^{-1}\mathfrak{p}$ is either the unit ideal, or is prime. The former holds iff $S \cap \mathfrak{p} \neq \emptyset$.

It follows that every prime ideal $\mathfrak{p}$ which does not meet S gives rise to a prime ideal $S^{-1}\mathfrak{p}$, and moreoever $(S^{-1}\mathfrak{p})^c = \mathfrak{p}$. The inclusion $\supseteq$ is clear, so let us prove $\subseteq$. Suppose x belongs to the left hand side. Then there exists $p \in \mathfrak{p}$ and $s \in S$ such that $x/1 = p/s$, and thus there exists $t \in S$ with $t(sx - p) = 0$. But then $(ts)x \in \mathfrak{p}$. Since $S \cap \mathfrak{p} = \emptyset$, this means that $x \in \mathfrak{p}$, as desired.

Putting these remarks together, the proposition is now proved. □

6.5. **Krull-Cohen-Seidenberg Theorems.** The following ultra-slick treatment of these theorems is taken from lectures of R. Swan. These theorems can be proved from what we have established about integral extensions, using localization as a tool. This is what is done in Atiyah-Macdonald. The point here is to show how localization may be avoided, and in fact the proof we will give is about as elementary as can be expected.

Theorem 6.5.1. *Let $A \subset B$ be an integral extension. Let $\mathfrak{p} \subset A$ be a prime ideal. Then an ideal P of B is a prime ideal with $P \cap A = \mathfrak{p}$ if and only if P is maximal among the ideals such that $P \cap A \subset \mathfrak{p}$.*

Proof. The last condition says P is maximal with respect to $P \cap S = \emptyset$, where $S = A - \mathfrak{p}$. Such an ideal is automatically prime (check this!), so in either case P will be prime.

Now suppose that P is prime and has $P \cap A = \mathfrak{p}$, but is not maximal among the ideals with $P \cap A \subset \mathfrak{p}$; then there exists an ideal $Q \supsetneq P$ with $Q \cap A = \mathfrak{p}$. Working mod P we can assume $P = \mathfrak{p} = 0$, and that B is a domain. Suppose $b \in Q$, $b \neq 0$, and let $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ be an equation for b over A of least degree n. Then $a_0 \neq 0$ since B is a domain. But then $a_0 \in Q \cap A = \mathfrak{p}$, contradicting the fact that $\mathfrak{p} = 0$.

Conversely, suppose that P is maximal with the property $P \cap A \subset \mathfrak{p}$. Working mod P we can assume $P = 0$. We must show that $\mathfrak{p} = 0$. Suppose that there is an element $a \in \mathfrak{p}$, $a \neq 0$. We claim that $(Ba) \cap A \subset \mathfrak{p}$, contradicting the maximality

of P. Indeed, suppose $ba \in (Ba) \cap A$. Let $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ be an equation for b over A. Then $(ab)^n + aa_{n-1}(ab)^{n-1} + \cdots + a^n a_0 = 0$, showing that $(ab)^n \in Aa \subset \mathfrak{p}$, so that $ab \in \mathfrak{p}$. □

The following three important results are immediate from Theorem 6.5.1.

Corollary 6.5.2 (Lying Over Theorem)**.** *If $A \subset B$ is an integral extension, then* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective.*

When $\mathfrak{q}^c = \mathfrak{p}$, we says that $\mathfrak{q}$ **lies over** $\mathfrak{p}$.

Corollary 6.5.3. *Let $A \subset B$ be an integral extension. Let $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = (\mathfrak{q}')^c =: \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Geometrically, this says that "if $i : A \hookrightarrow B$ is an integral extension, then there are no containments in the fibers of $i^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$".

Corollary 6.5.4 (Going Up Theorem)**.** *Let $A \subset B$ be an integral extension. If $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals in A, and $\mathfrak{q}$ is a prime ideal in B lying over $\mathfrak{p}$, then there exists a prime ideal $\mathfrak{q}'$ lying over $\mathfrak{p}'$, and with $\mathfrak{q} \subset \mathfrak{q}'$.*

Proof. Note that $\mathfrak{q} \cap A \subset \mathfrak{p}'$; choose an ideal $\mathfrak{q}'$ which is maximal among those which contain $\mathfrak{q}$ and have $\mathfrak{q}' \cap A \subset \mathfrak{p}'$. By Theorem 6.5.1, we have $\mathfrak{q}'$ is prime, and $\mathfrak{q}' \cap A = \mathfrak{p}'$. □

7. Lecture 7

7.1. Dimension is invariant under formation of integral extensions.

Proposition 7.1.1. *If $A \subset B$ is an integral extension, then* $\dim(A) = \dim(B)$.

Proof. If $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ is a chain of prime ideals in B, then the chain $P_0 \cap A \subsetneq P_1 \cap A \subsetneq \cdots \subsetneq P_n \cap A$ has the same length, by Corollary 6.5.3. If $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain of prime ideals in A, then we can lift it to a chain $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ in B, using the Lying Over Theorem to lift $\mathfrak{p}_0$ and then using the Going Up Theorem repeatedely to lift $\mathfrak{p}_i$, for $i > 0$. □

7.2. Going Down Theorem.

Theorem 7.2.1 (Going Down Theorem)**.** *Let $A \subset B$ be an integral extension. Assume that A is a normal domain and that B is torsion-free as an A-module. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and $P \in \mathrm{Spec}(B)$ with $P \cap A = \mathfrak{p}$. Let $\mathfrak{q} \in \mathrm{Spec}(A)$ with $\mathfrak{q} \subset \mathfrak{p}$. Then there is a prime $Q \in \mathrm{Spec}(B)$ with $Q \subset P$ and $Q \cap A = \mathfrak{q}$.*

For the proof we need two lemmas.

Lemma 7.2.2. *Let A be a normal domain with* $\mathrm{Frac}(A) = K$. *Let $f, g \in K[X]$ be monic. If $fg \in A[X]$, then $f \in A[X]$.*

Proof. The roots of f, being roots of fg are integral over A. Therefore so are the coefficients of f, but these are in K, hence in A since A is normal. □

Lemma 7.2.3. *Let $A \subset B$ be an integral extension and let $I \subset A$ be an ideal. Let $\widetilde{I} = \{x \in B \mid x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, for some n and $a_i \in I\}$. Then $\widetilde{I} = \sqrt{BI}$.*

Proof. It is clear that $\widetilde{I} \subset \sqrt{BI}$. For the converse, let $x^n = \sum_i b_i c_i$ with $b_i \in B$ and $c_i \in I$, for $i = 1, \ldots, r$. Then $C := B[b_1, \ldots, b_r]$ is finite over A and $x^n C \subset IC$. Now in Lemma 2.1.1, take $M = C$ and $\phi =$ mult. by x^n, to conclude that x satisfies an equation of the required form, so that $x \in \widetilde{I}$. □

Corollary 7.2.4. *Let $A \subset B$ be an integral extension. Assume A is a normal domain and B is torsion-free as an A-module. Let $K = \mathrm{Frac}(A)$, and $I \subset A$ be a prime ideal. Let $b \in B$. Then $b \in \sqrt{BI}$ iff the minimal polynomial f of b over K has the form $f = X^n + a_1 X^{n-1} + \cdots + a_n$ where all a_i lie in I.*

Proof. Suppose that $b \in \sqrt{BI}$. By Lemma 7.2.3, $b \in \widetilde{I}$, so that b is a root of a polynomial of form $h = X^k + q_1 X^{k-1} + \cdots + q_k$ with the $q_i \in I$. Since f is the minimal polynomial we have $h = fg$ in $K[X]$. By Lemma 7.2.2, f and g lie in $A[X]$. Modulo I, $\overline{f}\,\overline{g} = \overline{h} = \overline{X}^k$. Therefore, since I is prime, $\overline{f} = \overline{X}^n$ for some $n \leq k$ and f has the form $f = X^n + a_1 X^{n-1} + \cdots + a_n$, with the $a_i \in I$.

Conversely, note that $f(b) = 0$ holds in $K \otimes_A B$ (by *definition*, f is the minimal polynomial of b over K if it is the monic of least degree in $K[X]$ such that $f(b) = 0$ in $K \otimes_A B$). But then since B is torsion-free as an A-module, we have $f(b) = 0$ in B as well, so that $b \in \widetilde{I}$. Then by Lemma 7.2.3, $b \in \sqrt{BI}$, as desired. □

Proof of Theorem 7.2.1: It will suffice to show that if $S := (A - \mathfrak{q})(B - P)$, then $B\mathfrak{q} \cap S = \emptyset$. Why? In that case we can choose $Q \supset B\mathfrak{q}$ maximal with respect to $Q \cap S = \emptyset$. Then it follows (check this!) that Q is a prime ideal contained in P, such that $Q \cap A = \mathfrak{q}$.

Suppose that $s \in A - \mathfrak{q}$ and $t \in B - P$, and $st \in B\mathfrak{q}$. By Corollary 7.2.4, the minimal polynomial f of st over K is of the form $f = X^n + q_1 X^{n-1} + \cdots + q_n$, with the q_i in $\mathfrak{q}$. Since $s \in K - 0$, the minimal polynomial g of t over K has the form $g = X^n + a_1 X^{n-1} + \cdots + a_n$, where $q_i = s^i a_i$ for all i. By applying Corollary 7.2.4 (with $I = A$; note that that Corollary does hold true for $I = A$) to $b = t$, we see that all the a_i lie in A. Since $s \in A - \mathfrak{q}$, we have $a_i \in \mathfrak{q}$. By Corollary 7.2.4 again, $t \in \sqrt{B\mathfrak{q}}$. Since $B\mathfrak{q} \subset P$, it follows that $t \in P$, which is impossible. □

7.3. **Application of Going Down.**

Theorem 7.3.1. *Let A be a domain which is a f.g. k-algebra. Then all maximal chains of prime ideals in A have length equal to* $\mathrm{tr.deg}_k A$.

In particular, $\dim(A) = \mathrm{tr.deg}_k A$.

First we need to review the notion of transcendence degree. If $F \supset k$ is a field, and $B \subset F$ is a subset, let $k(B) \subset F$ be the subfield of F generated by k and B (= the smallest subfield that contains k, B). We say that B is a **transcendence basis** provided that

- The set B is algebraically independent over k, and
- F is an algebraic extension of $k(B)$.

Fact: Any extension of fields F/k has a transcendence basis B, and any two such bases have the same cardinality.

Note that $B = \emptyset$ iff F/k is algebraic. If $F = k(B)$, we say F/k is **purely transcendental**.

For the proof of the fact, see *N. Jacobson, Basic Algebra II, section 8.12.* We then define $\mathrm{tr.deg}_k F = |B|$, the cardinality of any transcendence basis. If A is a k-algebra domain with fraction field K, we define $\mathrm{tr.deg}_k A = \mathrm{tr.deg}_k K$.

To prove the theorem, we need the following lemma. We say a prime $P \in \mathrm{Spec}(A)$ has **height n** if

$$\sup\{k \mid \exists P_k \subsetneq P_{k-1} \subsetneq \cdots \subseteq P_0 = P\} = n.$$

(The number on the LHS is called simply $\mathrm{ht}(P)$.)

Lemma 7.3.2. *Let A be a domain which is a f.g. k-algebra. Let P be a prime ideal of height 1 in A (since A is a domain, this is just a minimal non-zero prime ideal). Then* $\mathrm{tr.deg}_k A/P = \mathrm{tr.deg}_k A - 1$.

Proof. Choose $k[x_1, \ldots, x_t] \subset A$ as in the Noether Normalization theorem. Then $t = \mathrm{tr.deg}_k A$. By Corollary 6.5.3, $P \cap k[x_1, \ldots, x_t] \neq 0$. Let $f \in P \cap k[x_1, \ldots, x_t]$ with $f \neq 0$. After using a substitution of variables as in the proof of Noether Normalization, we may assume f is monic in x_t (replace the x_i with $y_i := x_i + x_t^{m_i}$ if $i < t$, and $y_t := x_t$, for some large integers m_i). Therefore $k[x_1, \ldots, x_t]$ is integral over $k[x_1, \ldots, x_{t-1}, f]$, and we may replace x_t by f. Then we can assume $x_t \in \mathfrak{p} := P \cap k[x_1, \ldots, x_t]$. If $\mathfrak{p} \neq x_t k[x_1, \ldots, x_t]$, then the Going Down theorem shows that we can find $Q \subsetneq P$ in A with $Q \cap k[x_1, \ldots, x_t] = x_t k[x_1, \ldots, x_t]$, which would contradict the fact that P has height 1. So $\mathfrak{p} = x_t k[x_1, \ldots, x_t]$, so $k[x_1, \ldots, x_{t-1}] = k[x_1, \ldots, x_t]/x_t k[x_1, \ldots, x_t] \subset A/P$. Since this is an integral extension, $\mathrm{tr.deg}_k A/P = t - 1$, as required. □

Proof of Theorem 7.3.1: We use induction on $d = \mathrm{tr.deg}_k A$. If $d = 0$, then A is a field, which has dimension zero.

Suppose $d > 0$ and let $0 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ be a maximal chain of prime ideals in A. Then $0 = P_1/P_1 \subsetneq P_2/P_1 \subsetneq \cdots \subsetneq P_n/P_1$ is a maximal chain of prime ideals in $A' = A/P_1$. By Lemma 7.3.2, $\mathrm{tr.deg}_k A' = d - 1$, and so $n - 1 = d - 1$ by our induction hypothesis applied to A'. □

7.4. **Some counterexamples.** In the theorem, it is essential that A is a domain. What happens if we allow A to be more general? It is easy to see that if $A = k[X, Y] \times k[Z]$, then we have a maximal chain of prime ideals in the first factor having length 2, and a maximal chain of primes ideals in the second factor having length 1. In this case, the space $\mathrm{Spec}\, A$ is disconnected, and in fact is the disjoint union $\mathrm{Spec}(k[X, Y]) \coprod \mathrm{Spec}(k[Z])$ (see Atiyah-Macdonald, Ch. 1, Ex. 22), so it is not surprising that it is made up of "pieces with different dimensions".

How about if we avoid such silly examples by requiring A to be such that $\mathrm{Spec}\, A$ is connected, but not necessarily irreducible? Can we still have irreducible components that have different dimensions? The answer is yes, and an example has already been provided. Namely, recall the ring $A = k[X, Y, Z]/(XY, YZ)$. As we saw in Lecture 4, the corresponding variety is connected, a union of a line and a plane, which clearly have different dimensions. Algebraically, note that $I = (Y)(X, Z) = (Y) \cap (X, Z)$, a radical ideal since (Y) and (X, Z) are both prime. It follows that (Y) and (X, Z) are the only two minimal primes among those which contain I, which corresponds to the fact that there are two irreducible components in $\mathrm{Spec}(k[X, Y, Z]/I)$. Note that (Y) is the bottom prime in a chain of length two, and (X, Z) is the bottom prime in a chain of length one. This corresponds to the statement that $\dim(V(Y)) = 2$ and $\dim(V(X, Z)) = 1$, as we already knew since the first is the XZ-plane, and the second is the Y-axis.

7.5. **Returning to Geometric version of Noether Normalization.** In particular, Theorem 7.3.1 says that $\dim(k[X_1, \ldots, X_n]) = n$, as we claimed earlier. Moreover, in the geometric version of Noether normalization (Theorem 3.7.1), we claimed that $t = \dim(A)$, where t was the total number of algebraically independent elements $x_1, \ldots, x_t$ in $k[x_1, \ldots, x_t] \subset A$. This now follows from Lemma 7.1.1.

We have also justified that the map $\operatorname{Spec} A \to \operatorname{Spec}(k[x_1, \ldots, x_t])$ is surjective. We have *not* yet shown that the fibers are finite sets, although that is true.

7.6. **Hypersurfaces.** The following statement appears in Hartshorne's *Algebraic Geometry*, Prop. 1.13. We will prove it later, using the Krull Hauptidealsatz and a few other facts.

Proposition 7.6.1 (Codimension 1 subschemes in affine space)**.** *Then an irreducible closed subset $Y \subset \mathbb{A}^n_k = \operatorname{Spec}(k[X_1, \ldots, X_n])$ has dimension $n-1$ if and only if $Y = V(f)$, for some non-constant irreducible polynomial $f \in k[X_1, \ldots, X_n]$.*

Now here is a very interesting exercise, which you should compare with the above statement. How are they related?

Exercise 7.6.2. *Suppose k is a field which is NOT algebraically closed. Show that if $Z \subset k^n$ is a non-empty Zariski-closed subset (the set of zeros in k^n of an ideal $I \subset k[X_1, \ldots, X_n]$), then there is a single polynomial $f \in k[X_1, \ldots, X_n]$ such that $Z = Z(f)$, the set of zeros of f in k^n.*

Hint: It is enough to show that for any $m \geq 1$, there is a polynomial ϕ in m variables such that the only zero of ϕ in k^m is $(0, 0, \ldots, 0)$. (Then, if $Z = Z(I)$ where $I = (f_1, \ldots, f_m)$, we can put $f = \phi(f_1, \ldots, f_m)$.) Prove that ϕ exists, by first looking at the case $m = 2$.

8. Lecture 8

Categories and functors. Presheaves and sheaves. Stone-Cech theorem. Motivation for locally ringed spaces.

9. Lecture 9

Stalks, definition of locally ringed space. Examples. Definition of $\mathcal{O}_{\operatorname{Spec}(A)}$, and basic properties.

10. Lecture 10

Definition of affine scheme, and definition of scheme. Description of category of (affine) algebraic varieties in scheme-theoretic language. Example (deformations). DVRs; examples. Valuation rings. Basic properties.

11. Lecture 11

Recap of Noetherian rings/modules. Basic proposition. Proof E. Noether's theorem in invariant theory. Alternate proof of Nullstellensatz via basic proposition.

12. Lecture 12

We shall follow the treatment of associated primes and primary decompositions from [Mat2], Chapter 2, §6. You can find similar theorems (just for rings, not modules), in Atiyah-Macdonald, Chapter 4.

12.1. **Associated primes.** Throughout, we assume $A \neq 0$. We say an ideal $\mathfrak{q} \subset A$ is **primary** provided that $A/\mathfrak{q} \neq 0$ and every zero-divisor in $A/\mathfrak{q}$ is nilpotent. Equivalently, $\mathfrak{q} \neq A$, and

$$xy \in \mathfrak{q} \implies y \in \mathfrak{q} \text{ or } x^n \in \mathfrak{q} \text{ for some } n \geq 1.$$

If $I \subset A$ is an ideal, we say it has a **primary decomposition** if we can write $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ for some primary ideals $\mathfrak{q}_i$. We shall prove that when A is Noetherian, every ideal $I \subset A$ possesses a primary decomposition, and in that case there are various uniqueness statements one can make. In fact, following [Mat2], we shall actually prove analogous statements for all f.g. modules over A.

Fix an A-module M. Define

$$\mathrm{Ass}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} = \mathrm{ann}(x), \text{ for some } x \in M\}.$$

We call this the set of **associated primes** (to M). Note that $\mathfrak{p} \in \mathrm{Ass}(M)$ iff M contains a submodule isomorphic to $A/\mathfrak{p}$.

We say $a \in A$ is a **zero-divisor for** M if $\exists x \neq 0$ in M such that $ax = 0$.

We say $a \in A$ is M-**regular** if it is not a zero-divisor for M.

Lemma 12.1.1. *Let A be a Noetherian ring, and $M \neq 0$ an A-module.*

(a) *Every maximal element in the family $\mathcal{F} := \{\mathrm{ann}(x) \mid 0 \neq x \in M\}$ belongs to $\mathrm{Ass}(M)$. In particular, $\mathrm{Ass}(M) \neq \emptyset$.*

(b) *$\{$zero-divisors for $M\} = \cup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$.*

Proof. First note that since A is Noetherian, any non-empty family of ideals (such as $\mathcal{F}$) possesses maximal elements.
(a): If $\mathrm{ann}(x)$ is a maximal element of $\mathcal{F}$, then $\mathrm{ann}(x)$ is prime: $abx = 0$ and $bx \neq 0$ and $\mathrm{ann}(x) \subseteq \mathrm{ann}(bx)$ implies by maximality that $\mathrm{ann}(x) = \mathrm{ann}(bx)$, hence that $ax = 0$.
(b): The inclusion $\supseteq$ is clear. Let's prove $\subseteq$. Suppose $x \neq 0$ and $ax = 0$. Then a belongs to some maximal element of $\mathcal{F}$, hence a belongs to the right hand side. □

Lemma 12.1.2. *If*

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

is an exact sequence of A-modules, then $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

Proof. Let $\mathfrak{p} \in \mathrm{Ass}(M)$. Then $A/\mathfrak{p} \cong N$, for some submodule $N \subset M$. Note that $\mathfrak{p} = \mathrm{ann}(x)$ for any $0 \neq x \in N$ (since $\mathfrak{p}$ is prime). So if $N \cap M' \neq 0$, there exists $0 \neq x' \in M'$ with $\mathfrak{p} = \mathrm{ann}(x')$, so that $\mathfrak{p} \in \mathrm{Ass}(M')$.

On the other hand, if $N \cap M' = 0$, then N maps isomorphically onto its image in M'', and so the latter contains a copy of $A/\mathfrak{p}$; hence in that case $\mathfrak{p} \in \mathrm{Ass}(M'')$. □

Lemma 12.1.3. *Let A be Noetherian, and $M \neq 0$ a f.g. A-module. Then there exists a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of submodules such that for each i, $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$.*

Proof. Choose any $\mathfrak{p}_1 \in \mathrm{Ass}(M)$. Then M_1 exists with $M_1 \cong A/\mathfrak{p}_1$. If $M = M_1$, we are done. If $M_1 \neq M$, apply this to M/M_1. Repeat to find the desired chain. It terminates at M in finitely many steps, since M is Noetherian. □

For the next theorem, we need the notion of **support** $\mathrm{Supp}(M)$ of an A-module M. By definition

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\}.$$

Lemma 12.1.4. *M a finite A-module $\implies$ $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$, a Zariski-closed subset of $\mathrm{Spec}(A)$.*

Proof. Write $M = Am_1 + \cdots + Am_n$. Fix $\mathfrak{p} \in \mathrm{Spec}(A)$. Then

$$\begin{aligned} M_{\mathfrak{p}} \neq 0 &\Leftrightarrow \exists i \text{ with } m_i \neq 0 \text{ in } M_{\mathfrak{p}} \\ &\Leftrightarrow \exists i \text{ with } \mathrm{ann}(m_i) \subset \mathfrak{p} \\ &\Leftrightarrow \mathrm{ann}(M) = \cap_i \mathrm{ann}(m_i) \subset \mathfrak{p}. \end{aligned}$$

In the last $\Leftrightarrow$, $\Rightarrow$ is clear. For $\Leftarrow$, use the exercise below. □

Exercise 12.1.5. *If P is prime and $P \supset \cap_{i=1}^n \mathfrak{a}_i$ for some ideals $\mathfrak{a}_i$, then there exists some j such that $P \supset \mathfrak{a}_j$.*

Now we can state and prove the following fundamental result.

Theorem 12.1.6. *Let A be Noetherian, and M a f.g. A-module. Then*

1. *$\mathrm{Ass}(M)$ is a finite set.*
2. *$\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$.*
3. *The minimal elements of $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ coincide.*

Proof. (1): By Lemma 12.1.3 there is a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that $M_i/M_{i-1} = A/\mathfrak{p}_i$. Now Lemma 12.1.2 (and induction) shows that

$$\mathrm{Ass}(M) \subset \cup_i \mathrm{Ass}(A/\mathfrak{p}_i) = \{\mathfrak{p}_i\}_i.$$

This shows that $\mathrm{Ass}(M)$ is finite.
(2): If $0 \to A/\mathfrak{p} \to M$ is exact, then so is $0 \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \to M_{\mathfrak{p}}$, in which case $M_{\mathfrak{p}} \neq 0$.
(3): First, we need a "localyzing lemma" for the behavior of Ass. In this proof, we use the following notation: $M_S := S^{-1}M$, and $A_S := S^{-1}A$, for any multiplicative set $S \subset A$.

Lemma 12.1.7. (a) *If $N \in A_S$-mod, then $\mathrm{Ass}_{A_S}(N) = \mathrm{Ass}_A(N)$ (via the identification $\mathrm{Spec}(A_S) \subset \mathrm{Spec}(A)$).*
(b) *Suppose A is Noetherian and $M \in A$-mod. Then $\mathrm{Ass}(M_S) = \mathrm{Ass}(M) \cap \mathrm{Spec}(A_S)$.*

In particular, if A is Noetherian, $\mathfrak{p} \in \mathrm{Ass}_A(M) \Leftrightarrow \mathfrak{p}A_{\mathfrak{p}} \in \mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$.

Proof. Note that the last statement is an immediate consequence of (a),(b).
(a): Let $x \in N$. We have $\mathrm{ann}_A(x) = \mathrm{ann}_{A_S}(x) \cap A$. So $P \in \mathrm{Ass}_{A_S}(N) \implies \mathfrak{p} := P \cap A \in \mathrm{Ass}(N)$.

Conversely, if $\mathfrak{p} \in \mathrm{Ass}_A(N)$ and $x \in N$ is such that $\mathfrak{p} = \mathrm{ann}_A(x)$, then $x \neq 0$ hence $\mathfrak{p} \cap S = \emptyset$. Hence $P = \mathfrak{p}A_S$ is a prime ideal such that $P = \mathrm{ann}_{A_S}(x)$.
(b): If $\mathfrak{p} \in \mathrm{Ass}(M) \cap \mathrm{Spec}(A_S)$, then $\mathfrak{p} \cap S = \emptyset$ and $\mathfrak{p} = \mathrm{ann}_A(x)$, for some $x \in M$. If $(a/s)x = 0$ then $\exists t \in S$ such that $tax = 0$; $t \notin \mathfrak{p}, ta \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$. Hence $\mathrm{ann}_{A_S}(x) = \mathfrak{p}A_S$, and so $\mathfrak{p}A_S \in \mathrm{Ass}(M_S)$.

Conversely, if $P \in \mathrm{Ass}(M_S)$, then WLOG $P = \mathrm{ann}_{A_S}(x)$, for $x \in M$. If $\mathfrak{p} := P \cap A$, we have $P = \mathfrak{p}A_S$ and $\mathfrak{p} \cap S = \emptyset$.
Claim: $\exists t \in S$ such that $\mathfrak{p} = \mathrm{ann}_A(tx)$, hence $\mathfrak{p} \in \mathrm{Ass}(M) \cap \mathrm{Spec}(A_S)$.
Proof of Claim: $\mathfrak{p}$ is a f.g. ideal, say by $f_1, \ldots, f_n$. Now $f_i x = 0$ in M_S implies that $\exists t_i \in S$ such that $f_i t_i x = 0$ in M. Take $t = t_1 \cdots t_n$. This does the job, and the

claim is proved. To see why, note that

$$\mathfrak{p} \subset \mathrm{ann}_A(tx) \subset \mathrm{ann}_{A_S}(tx) \cap A = \mathrm{ann}_{A_S}(x) \cap A = \mathfrak{p},$$

proving that $\mathfrak{p} \in \mathrm{Ass}(M) \cap \mathrm{Spec}(A_S)$.

We have proved the lemma. □

Now we finish the proof of the theorem by proving part (3). It's ETS [3] that a minimal element of $\mathrm{Supp}(M)$ belongs to $\mathrm{Ass}(M)$. Let $\mathfrak{p}$ be such an element.

Using Lemma 12.1.7, we have

$$\begin{aligned} 0 \neq M_{\mathfrak{p}} \Rightarrow \emptyset \neq \mathrm{Ass}(M_{\mathfrak{p}}) &= \mathrm{Ass}(M) \cap \mathrm{Spec}(A_{\mathfrak{p}}) \\ &\subset \mathrm{Supp}(M) \cap \mathrm{Spec}(A_{\mathfrak{p}}) \\ &= \{\mathfrak{p}\}. \end{aligned}$$

So $\mathfrak{p} \in \mathrm{Ass}(M_{\mathfrak{p}})$, and hence $\mathfrak{p} \in \mathrm{Ass}(M)$, as desired. □

12.2. **Consequences.** Let A be a Noetherian ring, and M a f.g. A-module.

- Let $\{P_i\}_{i=1}^r$ be the set of minimal elements of $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$, or equivalently the set of minimal elements of $\mathrm{Ass}(M)$ (the set is finite since $\mathrm{Ass}(M)$ is finite). Then $V(\mathrm{ann}(M)) = V(P_1) \cup \cdots \cup V(P_r)$. In other words, the $V(P_i)$'s are precisely the irreducible components of the closed set $V(\mathrm{ann}(M))$.

  We call the primes P_i here the **isolated primes** of M. We call the remaining primes of $\mathrm{Ass}(M)$, the **embedded primes** of M.
- Letting $M = A/I$, we see in particular that there are only finitely many minimal prime ideals containing I. Furthermore, in this case we have

  $$\mathrm{Ass}(A/I) = \{P \in \mathrm{Spec}(A) \mid \exists x \in A \,\text{such that}\, P = (I : x)\ \}.$$

  Here for any subset $J \subset A$, we define the ideal $(I : J) = \{a \in A \mid aJ \subset I\}$. Thus, $\mathrm{Ass}(A/I)$ is precisely the set

  $$\mathrm{Ass}(A/I) = \{\text{the ideals } (I : x),\ x \in A,\ \text{which are prime}\}.$$
- Suppose A is reduced. Then $\mathrm{Ass}(A)$ is precisely the set of minimal primes $P_1, \ldots P_r$ of A. Since every minimal prime ideal of A is associated (Theorem 12.1.6), we need only show that every associated prime is one of the P_i's. To prove this note that, A being reduced, we have a canonical inclusion

  $$A = \frac{A}{P_1 \cap \cdots \cap P_r} \hookrightarrow \oplus_i A/P_i,$$

  and thus

  $$\mathrm{Ass}(A) \subset \cup_i \mathrm{Ass}(A/P_i) = \{P_i\}_i.$$

13. Lecture 13

13.1. **Primary submodules.** Let $N \subset M$ be a submodule of the A-module M. We say N is **primary** if $N \neq M$ and if the following property holds: if $a \in A$ is a zero-divisor of M/N, then $a \in \sqrt{\mathrm{ann}(M/N)}$. Equivalently, for all $a \in A, x \in M$, we have

$$x \notin N \text{ and } ax \in N \implies a^\nu M \subset N \text{ for some } \nu \geq 1.$$

The primary submodules of $M = A$ are precisely the primary ideals of A.

[3] Enough To Show

The following theorem gives us a crucial characterization of primary submodules as exactly those N for which $\mathrm{Ass}(M/N)$ is a singleton.

Theorem 13.1.1. *Suppose M is a f.g. A-module, and $N \subset M$ is a submodule. Then*

$$N \subset M \text{ is primary } \Leftrightarrow \mathrm{Ass}(M/N) = \{P\},$$

in which case $I := \mathrm{ann}(M/N)$ is primary and $\sqrt{I} = P$.

Corollary 13.1.2. *$I \subset A$ is primary iff $\exists!\, P$ of the form $P = (I : x)$, and in that case $\sqrt{I} = P$.*

The corollary is an immediate consequence of the theorem. Let us now prove the theorem.

Proof. ($\Leftarrow$): We have $\mathrm{Supp}(M/N) = V(P) = V(\mathrm{ann}(M/N))$, and so $P = \sqrt{\mathrm{ann}(M/N)}$. Now $a \in A$ is a zero-divisor for M/N implies $a \in P$ (use e.g. the proof of Lemma 12.1.1 to see that a belongs to an associated prime). So $N \subset M$ is primary.
($\Rightarrow$): Conversely, if $P \in \mathrm{Ass}(M/N)$ then every $a \in P$ is a zero-divisor for M/N, and so (by assumption that N is primary) $a \in \sqrt{\mathrm{ann}(M/N)}$. So $P \subset \sqrt{\mathrm{ann}(M/N)}$. But $\mathrm{ann}(M/N) \subset P$ (by definition of $\mathrm{Ass}(M/N)$), hence $P = \sqrt{\mathrm{ann}(M/N)}$, and $\mathrm{Ass}(M/N)$ consists of just one element, which is $P = \sqrt{\mathrm{ann}(M/N)}$.

Now that we have proved the equivalence $\Leftrightarrow$, we must verify
Claim: In this case, $I := \mathrm{ann}(M/N)$ is primary.
Proof: Suppose $a, b \in A,\ b \notin I$, and $ab \in I$. Then $ab(M/N) = 0$, but $b(M/N) \neq 0$. This implies that a is a zero-divisor for M/N, and thus (since N is primary) $a \in \sqrt{\mathrm{ann}(M/N)}$. Thus I is primary, as desired. □

If $\mathrm{Ass}(M/N) = \{P\}$, we say N is **P-primary**, or a **primary submodule belonging to** P.

Corollary 13.1.3. *If $I \subset A$ has $\sqrt{I} = \mathfrak{m}$, a maximal ideal of A, then I is $\mathfrak{m}$-primary.*

Proof. It's ETS that if $P = (I : x)$ is prime, then $P = \mathfrak{m}$. But $P = (I : x) \supset I$, hence $P = \sqrt{P} \supset \sqrt{I} = \mathfrak{m}$, which proves that $P = \mathfrak{m}$. □

Example. Let k be a field, and let $A = k[X, Y, Z]/(XY - Z^2)$. Let x, y, z denote the images of $X, YZ \in k[X, Y, Z]$ in A. Let $\mathfrak{p} := (x, z) \subset A$. Note that

- $\mathfrak{p}$ is prime: $A/\mathfrak{p} \cong k[Y]$;
- $\sqrt{\mathfrak{p}^2} = \mathfrak{p}$;
- $\mathfrak{p}^2$ is not primary: $xy = z^2 \in \mathfrak{p}^2$, yet $x \notin \mathfrak{p}^2$ and $y \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$.

Hence $\sqrt{I}$ being *prime* is not sufficient to guarantee that I is primary.

13.2. **Various definitions relating to primary decompositions.** Our goal is to investigate when a submodule $N \subset M$ can be written in the form $N = N_1 \cap \cdots \cap N_r$, for some primary submodules $N_i \subset M$. We call such an expression a **primary decomposition** of N. The following lemma says that we may as well "group together" the N_i's which belong to the same prime (i.e. if certain terms N_{i_j} all belong to P_i, in the primary decomposition we denote the intersection $\cap_j N_{i_j}$ simply by the symbol N_i). In this way, we can assume that the N_i's in a primary decomposition belong to *distinct* prime ideals.

Lemma 13.2.1. *If $N, N' \subset M$ are P-primary submodules, then so is $N \cap N'$.*

Proof. We have an inclusion

$$\frac{M}{N \cap N'} \hookrightarrow \frac{M}{N} \oplus \frac{M}{N'},$$

and thus $\mathrm{Ass}(M/(N \cap N') \subset \mathrm{Ass}(M/N) \cup \mathrm{Ass}(M/N') = \{P\}$, which implies the result. □

The above will be exploited in proving a kind of *uniqueness* result for primary decompositions. What about *existence*? This will be done using the following notions.

We say $N \subset M$ is **reducible** if $N = N_1 \cap N_2$ for submodules N_i with $N \subsetneq N_i$, $i = 1, 2$. We say N is **irreducible** provided it is not reducible.

Lemma 13.2.2. *Suppose M is Noetherian. Then any submodule N is an intersection of finitely many irreducible submodules.*

Proof. Consider the family $\mathcal{F} := \{N \subset M \mid N \text{ has no such expression}\}$. We assume $\mathcal{F} \neq \emptyset$ and derive a contradiction.

Choose a maximal element $N_0 \in \mathcal{F}$ (using that M is Noetherian). Then N_0 is reducible, so we may write it as $N_0 = N_1 \cap N_2$, where $N_0 \subsetneq N_i$, $i = 1, 2$. By maximality each N_i is an intersection of finitely many irreducible submodules; hence so is N_0. This is nonsense. □

We say an expression $N = N_1 \cap \cdots \cap N_r$ is **irredundant** if no N_i can be omitted. That is, for each i, we have $N_i \nsubseteq \cap_{j \neq i} N_j$. We thus have the notion of an irredundant primary decomposition $N = N_1 \cap \cdots \cap N_r$, an irredundant expression in which each N_i is P_i-primary, for a prime P_i.

In an irredundant primary decomposition, if we group together the N_{i_j}'s belonging to the same prime according to Lemma 13.2.1, and write their intersection as a single module, then we call the resulting expression a **shortest primary decomposition**. It has the property that $P_i \neq P_j$ if $i \neq j$. In that case, N_i is called "the" P_i-primary component of N (as we shall see below, sometimes N_i is indeed uniquely determined by P_i and N).

The following theorem is our main result concerning the existence and uniqueness of primary decompositions.

Theorem 13.2.3. *Let A be Noetherian, and let M be a finite A-module.*

(i) *Any irreducible submodule is primary.*
(ii) *If $N = N_1 \cap \cdots \cap N_r$, with $\mathrm{Ass}(M/N_i) = \{P_i\}$, is an irredundant primary decomposition of $N \subsetneq M$, then $\mathrm{Ass}(M/N) = \{P_1, \ldots, P_r\}$.*
(iii) *Ever proper submodule $N \subsetneq M$ has a primary decomposition. If P is a* minimal *element of $\mathrm{Ass}(M/N)$, then the P-primary component of N is $\phi_P^{-1}(N_P)$, where $\phi_P : M \to M_P$ is the canonical map (in particular the P-primary component is uniquely determined by M, N, P).*

14. Lecture 14

14.1. **Proof of Theorem 13.2.3.** (i): Assume N is not primary. Then by Theorem 13.1.1 there exist $P_1 \neq P_2$ in $\mathrm{Ass}(M/N)$. So we can find submodules $K_i \subset M/N$ where $K_i \cong A/P_i$, for $i = 1, 2$. But then $K_1 \cap K_2 = \overline{0}$ (since any $0 \neq x \in K_i$ has $\mathrm{ann}(x) = P_i$). This shows that N is reducible.

(ii): WLOG $N = 0$, and $0 = N_1 \cap \cdots \cap N_r$. Since $M \hookrightarrow \oplus_i M/N_i$, we have $\mathrm{Ass}(M) \subset \{P_1, \ldots, P_r\}$.

We want to prove that $P_1 \in \mathrm{Ass}(M)$ (the same argument applies to any other P_i). As $N_2 \cap \cdots \cap N_r \neq 0$, we may choose $0 \neq x \in N_2 \cap \cdots \cap N_r$, so that $\mathrm{ann}(x) = (0 : x) = (N_1 : x)$. But $(N_1 : M) = \mathrm{ann}(M/N_1)$ is a primary ideal with $\sqrt{(N_1 : M)} = P_1$, so $P_1^\nu M \subset N_1$ for some $\nu \geq 1$. Therefore $P_1^\nu x \subset N_1$ and thus $P_1^\nu x = 0$ for some $\nu \geq 1$. Choose $\nu \geq 0$ such that

$$P_1^\nu x \neq 0, \qquad P_1^{\nu+1} x = 0.$$

Let y be any non-zero element of $P_1^\nu x$, so that y satisfies

- $P_1 y = 0$, and so $P_1 \subset \mathrm{ann}(y)$;
- $y \in N_2 \cap \cdots \cap N_r$, and so $y \notin N_1$.

Since N_1 is primary, we see that $a \in \mathrm{ann}(y) \implies a \in \sqrt{\mathrm{ann}(M/N_1)} = P_1$. Thus in fact $P_1 = \mathrm{ann}(y)$, proving that $P_1 \in \mathrm{Ass}(M)$, as desired.

(iii): Every proper submodule N has an irreducible decomposition, hence a primary decomposition (by (i)). Let $N = N_1 \cap \cdots \cap N_r$ be a *shortest* primary decomposition. We want to prove that if, say, P_1 is minimal in $\mathrm{Ass}(M/N)$, then N_1 is determined by M, N, P_1.

Write P for P_1 from now on. Localizing, we get $N_P = (N_1)_P \cap \cdots \cap (N_r)_P$. Also, there is a $\nu > 0$ such that, for each $i > 1$, we have $P_i^\nu \subset \mathrm{ann}(M/N_i)$. Since we are assuming P is minimal in $\mathrm{Ass}(M/N)$, we have $P_i \not\subseteq P$ for $i > 1$. From these two remarks we see that $(M/N_i)_P = 0$ that is, $(N_i)_P = M_P$, for $i > 1$ (check this!).

It follows that $N_P = (N_1)_P$, and so $\phi_P^{-1}(N_P) = \phi_P^{-1}((N_1)_P) = N_1$, as desired. Let us check the non-trivial inclusion $\subseteq$ of this last equality more carefully. If $m \in \phi_P^{-1}((N_1)_P)$, then we may write $\frac{m}{1} = \frac{n_1}{s}$ for some $n_1 \in N_1$ and $s \in A - P$. There is then a $t \notin P$ such that $tm \in N_1$. Let $\overline{m} \in M/N_1$ denote the image of m. We see that $\exists t \notin P$ such that $t\overline{m} = 0$. If $\overline{m} \neq 0$, then the fact that N_1 is P-primary means that for $a \in A$, $a \in \mathrm{ann}(\overline{m}) \implies a \in \sqrt{\mathrm{ann}(M/N_1)} = P$. Applying this implication to $a = t$, we would have $t \in P$, a contradiction. It follows that $\overline{m} = 0$, i.e., $m \in N_1$. This shows $\phi_P^{-1}((N_1)_P) \subseteq N_1$, as desired. □

14.2. **Examples and applications.** The next corollary follows immediately from Theorem 13.2.3.

Corollary 14.2.1. *If A is a Noetherian ring, then every proper ideal I has a shortest primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. The set of ideals $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ to which the $\mathfrak{q}_i$'s belong is uniquely determined by I. The $\mathfrak{q}_i$'s belonging to* minimal *$\mathfrak{p}_i$'s are uniquely determined by I.*

The following example shows that an ideal may have two (or more) distinct shortest primary decompositions.

Example. In $k[X, Y]$, let $I = (X^2, XY) = (X) \cap (X, Y)^2 = (X) \cap (X^2, Y)$. Note that $(X, Y)^2$ and (X^2, Y) both have as radical the maximal ideal (X, Y), hence both are (X, Y)-primary. The ideal (X) is prime, hence primary. So, we have two distinct shortest primary decompositions for I. Note that $\mathrm{Ass}(A/I) = \{(X), (X, Y)\}$, so that (X) is isolated, and (X, Y) is embedded.

We can also use primary decompostions to prove the unique factorization of ideals in a Dedekind domain. We will prove in the next lecture the following proposition/definition which characterizes Dedekind domains.

Proposition 14.2.2. *Let A be a Noetherian domain with dimension 1. Then the following statements are equivalent.*

(1) *A is normal.*
(2) *Every primary ideal in A is a power of a prime ideal.*
(3) *Every localization $A_{\mathfrak{p}}$, for $\mathfrak{p} \neq 0$ a prime ideal, is a DVR.*

If A satisfies these properties, we call it a **Dedekind domain**.

Using this, we get the aforementioned unique factorization of ideals in A.

Corollary 14.2.3. *Suppose A is a Dedekind domain and I is a proper, non-zero ideal. Then $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ for a uniquely determined set of non-zero prime ideals $\mathfrak{p}_i$, and positive integers a_i, for $i = 1, \ldots, r$.*

Proof. By (2) above, the shortest primary decomposition takes the form $I = \mathfrak{p}_1^{a_1} \cap \cdots \cap \mathfrak{p}_r^{a_r}$ for distinct non-zero prime ideals $\mathfrak{p}_i$ and positive integers a_i. Since the dimension of A is 1, the $\mathfrak{p}_i$'s are in fact maximal ideals, hence are pairwise coprime: $\mathfrak{p}_i + \mathfrak{p}_j = A$, if $i \neq j$. Furthermore, this implies that $\mathfrak{p}_i^{a_i} + \mathfrak{p}_j^{a_j} = A$. From this it follows that the intersection is actually a product: $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ (for a proof, see Atiyah-Macdonald, Prop. 1.10). The uniqueness of this expression follows from the uniqueness statement in Corollary 14.2.1, since each $\mathfrak{p}_i$ is a minimal prime in $\mathrm{Ass}(A/I)$ (in fact since $\dim(A) = 1$, and $I \neq 0$, all primes containing I are minimal primes containing I). □

15. Lecture 15

Characterizations of DVR's, and applications to Dedekind domains (proofs). Characterization of normal rings.

15.1. **Characterizations of DVR's.** Let A denote a DVR with fraction field K, with valuation $v : K^\times \to \mathbb{Z}$. As usual set $v(0) = \infty$. Note the following two facts:

- The only non-zero ideals of A are the sets of the form $\mathfrak{m}_k := \{y \mid v(y) \geq k\}$. (Check this! Use that any ideal $\mathfrak{a} \neq 0$ possesses an element y with minimal valuation.) Thus, A Noetherian, as every ascending chain of ideals taken from the set $\mathfrak{m}_1 \supset \mathfrak{m}_2 \supset \cdots$ is stationary.
- The maximal ideal is $\mathfrak{m} = \mathfrak{m}_1$. We have $\mathfrak{m} = (x)$ for any element x satisfying $v(x) = 1$. In that case, we also have $\mathfrak{m}_k = (x^k)$, for all $k \geq 1$. So the only prime ideals are $\mathfrak{m}, (0)$; and so $\dim(A) = 1$.

Thus, any DVR is a Noetherian local domain of dimension 1, in which every ideal is principal. In fact this characterizes DVR's among all Noetherian local domains of dimension 1.

The following is Proposition 9.2 from Atiyah-Macdonald.

Proposition 15.1.1. *Let $(A, \mathfrak{m})$ be a Noetherian local domain of dimension 1, with residue field $k := A/\mathfrak{m}$. Then TFAE [4]:*

(i) *A is a DVR.*
(ii) *A is normal.*
(iii) *$\mathfrak{m}$ is principal.*
(iv) *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.*
(v) *Every non-zero ideal is $\mathfrak{m}^k$, for some $k \geq 0$.*

[4]The Following Are Equivalent

(vi) $\exists x \in A$ *such that every non-zero ideal is* (x^k)*, for some* $k \geq 0$.

Proof. Note that any ideal $\mathfrak{a} \neq (0), (1)$ is $\mathfrak{m}$-primary, hence $\mathfrak{a} \supset \mathfrak{m}^n$ for some $n \geq 1$. To see this, use that $\sqrt{\mathfrak{a}} = \mathfrak{m}$, since $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{a}$.

$(i) \implies (ii)$: Every valuation ring is normal (Lemma ????).

$(ii) \implies (iii)$: Assume $0 \neq a \in \mathfrak{m}$. Then $\exists n \geq 1$ such that $\mathfrak{m}^n \subset (a)$, but $\mathfrak{m}^{n-1} \not\subseteq (a)$. Choose $b \in \mathfrak{m}^{n-1} - (a)$, and set $x = a/b \in K$. We have $x^{-1} \notin A$ (since $b \notin (a)$), hence x^{-1} is not integral over A. Hence $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ (if $x^{-1}\mathfrak{m} \subset \mathfrak{m}$, then $\mathfrak{m}$ would be a faithful $A[x^{-1}]$-module, f.g. as an A-module, and thus x^{-1} would be integral). But $x^{-1}\mathfrak{m} \subset A$, hence $x^{-1}\mathfrak{m} = A$, and $\mathfrak{m} = (x)$.

$(iii) \implies (iv)$: Assume $\mathfrak{m} = (x)$. Clearly $\mathfrak{m}/\mathfrak{m}^2$ is generated by the image of x, hence its $\dim_k$ is ≤ 1. If the dimension is zero, then $\mathfrak{m} = \mathfrak{m}^2$ and NAK implies $\mathfrak{m} = 0$, a contradiction.

$(iv) \implies (v)$: $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ and NAK imply $\mathfrak{m} = (x)$ for some x. For an ideal $\mathfrak{a} \neq (0), (1)$, we can choose an integer $k > 0$ such that $\mathfrak{m} \supset \mathfrak{a} \supset \mathfrak{m}^k = (x^k)$.

Consider $\overline{\mathfrak{a}} \subset A/(x^k) =: \overline{A}$ (an Artinian ring). WLOG $\overline{\mathfrak{a}} \neq (\overline{x}^k)$. Since $\overline{x}$ is nilpotent, there exists r with $\overline{\mathfrak{a}} \subset (\overline{x}^r)$ and $\overline{\mathfrak{a}} \not\subseteq (\overline{x}^{r+1})$. Take $y \in \overline{\mathfrak{a}}$ with $y \notin (\overline{x}^{r+1})$. Note

$$\begin{aligned} y = \overline{u}\,\overline{x}^r &\Rightarrow \overline{u} \in \overline{A}^\times \\ &\Rightarrow \overline{x}^r \in \overline{\mathfrak{a}} \\ &\Rightarrow \overline{\mathfrak{a}} = (\overline{x}^r) \\ &\Rightarrow \mathfrak{a} = \mathfrak{m}^r = (x^r). \end{aligned}$$

This completes the proof.

$(v) \implies (vi)$: $\mathfrak{m} \neq \mathfrak{m}^2$ implies $\exists x \in \mathfrak{m} - \mathfrak{m}^2$. By hypothesis $(x) = \mathfrak{m}^r$ for some $r \geq 1$. But then we must have $r = 1$, so that $\mathfrak{m} = (x)$ and $\mathfrak{m}_k = (x^k)$ for all $k \geq 1$.

$(vi) \implies (i)$: Write $\mathfrak{m} = (x)$; note $(x^k) \neq (x^{k+1})$ for all $k \geq 0$. Take $a \in A - 0$, and write $(a) = (x^k)$, some $k \geq 0$. then $a \in A^\times x^k$.

Claim: $K^\times = \coprod_{k \in \mathbb{Z}} (A^\times x^k)$.

Proof: Given $\frac{a}{b} \in K^\times$, write $a = ux^k$ and $b = vx^m$, for $u, v \in A^\times$. Then $\frac{a}{b} = uv^{-1}x^{k-m}$.

Now, we can define a function $v : K^\times \to \mathbb{Z}$ by setting $v(ux^k) = k$. It is easy to see that v is a discrete valuation of K, with valuation ring A. Hence A is a DVR. □

15.2. **Proof of Proposition 14.2.2.** (1) $\iff$ (3): Use Proposition 15.1.1 above and the fact that "normality is a local property".

(2) $\iff$ (3): Use Proposition 15.1.1 and the fact, proved in Atiyah-Macdonald 4.8, that contraction of ideals gives a bijective correspondence

$$\{\text{primary ideas in } S^{-1}A\} \longleftrightarrow \{\text{contracted primary ideals in } A\},$$

and a similar one, where the word "primary" is replaced with "prime". □

15.3. **Improvement on** $(iii) \implies (vi)$ **in Proposition 15.1.1.** For later purposes, we need to give a proof of the implication $(iii) \implies (vi)$, *without the dimension 1 hypothesis.*

Proposition 15.3.1. *Suppose* $(A, \mathfrak{m})$ *is a Noetherian local domain in which* $\mathfrak{m}$ *is principal and non-zero. Then A is a PID (hence of dimension 1, hence a DVR).*

Proof. Write $\mathfrak{m} = (x)$. Consider the family $\mathcal{F} = \{\mathfrak{a} \subset A \mid \mathfrak{a} \text{ is not principal}\}$. We will assume $\mathcal{F} \neq \emptyset$, and derive a contradiction.

If $\mathcal{F} \neq \emptyset$, it contains a maximal element, say $\mathfrak{a}$. So $\mathfrak{a} \neq (0), (1), \mathfrak{m}$.

We will need the notion of invertible ideal. For any ideal $I \subset A$, define $I^{-1} := \{x \in K \mid xI \subset A\}$, otherwise known by the symbol $(A : I)$. By definition we have $I\, I^{-1} \subset A$. We say I is **invertible** if $I\, I^{-1} = A$. Note that every principal ideal is invertible.

Claim: $\mathfrak{a}$ is not invertible.

Proof: If $\mathfrak{a}\,\mathfrak{a}^{-1} = A$, then $\exists a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{a}^{-1}$ such that $\sum_i a_i b_i = 1$. At least one summand $a_i b_i \in A^\times$, and then

$$\mathfrak{a} = a_i b_i \mathfrak{a} \subset a_i A \subset \mathfrak{a},$$

so $\mathfrak{a} = (a_i)$, a contradiction. The claim is proved.

Now we know that $\mathfrak{a} \subset \mathfrak{m}$. Thus $\mathfrak{m}^{-1}\,\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\,\mathfrak{m} = A$ (if $\mathfrak{m}^{-1}\,\mathfrak{a} = A$, then $\mathfrak{a}^{-1} = \mathfrak{m}^{-1}$ and $\mathfrak{a}$ is invertible).

On the other hand, we know that $\mathfrak{a} = \mathfrak{m}^{-1}\,\mathfrak{m}\,\mathfrak{a} \subset \mathfrak{m}^{-1}\,\mathfrak{a}$. This leaves us only two options.

Case 1: $\mathfrak{a} = \mathfrak{m}^{-1}\,\mathfrak{a}$. Then $\mathfrak{m}\,\mathfrak{a} = \mathfrak{a}$, hence by NAK $\mathfrak{a} = (0)$, a contradiction.
Case 2: $\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\,\mathfrak{a}$. Then by choice of $\mathfrak{a}$ as a maximal element of $\mathcal{F}$, we know $\mathfrak{m}^{-1}\,\mathfrak{a}$ is principal, equal to (y), for some $y \in A$. But then $\mathfrak{a} = \mathfrak{m}\,(y) = (xy)$, a contradiction.

So, $\mathcal{F} \neq \emptyset$ leads to a contradiction in every case. □

15.4. **Characterization of normal domains.** The first step is the following proposition.

Proposition 15.4.1. *Let A be a Noetherian domain, and $P \neq 0$ a prime ideal. Then if P is invertible, then* $\mathrm{ht}(P) = 1$*, and A_P is a DVR.*

Proof. P invertible $\implies$ PA_P invertible $\implies$ (by proof of claim appearing in Proposition 15.3.1 above) PA_P is principal $\implies$ (by Proposition 15.3.1 itself) A_P has dim 1 and is a DVR, and $\mathrm{ht}(P) = 1$. □

Proposition 15.4.2. *Let A be a normal Noetherian domain. Then*

(i) *For all $P \in \mathrm{Ass}(A/(a))$, $((a) \neq (0))$, we have* $\mathrm{ht}(P) = 1$*, hence all such P's are isolated primes.*
(ii) $A = \bigcap_{\mathrm{ht}(P)=1} A_P$.

Proof. (i): Fix $a \neq 0$. If $P \in \mathrm{Ass}(A/(a))$, we can write $P = (aA : b)$, for some $b \in A$. Then

$$\mathfrak{m} := PA_P = (aA_P : b) = (A_P : ba^{-1}),$$

and thus $ba^{-1}\mathfrak{m} \subset A_P$ and $ba^{-1} \notin A_P$.

If $ba^{-1}\mathfrak{m} \subset \mathfrak{m}$, then ba^{-1} is integral over A_P, contradicting the normality of A_P. Hence $ba^{-1}\mathfrak{m} = A_P$, and so $\mathfrak{m}^{-1}\,\mathfrak{m} = A_P$. By Proposition 15.4.1, $\mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(P) = 1$.

(ii): It's ETS the following statement: if $a, b \in A$, $a \neq 0$ and $b \in aA_P$ for all P of ht 1, then $b \in aA$.

Consider a shortest primary decomposition $aA = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, where $P_i := \sqrt{\mathfrak{q}_i}$ for each i.

By (i), each P_i has ht 1. Therefore each P_i is minimal, and by the uniqueness statement in Corollary 14.2.1, each $\mathfrak{q}_i$ is uniquely determined. In fact, we have

$$\mathfrak{q}_i = A \cap aA_{P_i}.$$

Since b belongs to the intersection of all the terms on the RHS by hypothesis, it also belongs to $\cap_i \mathfrak{q}_i = aA$, as desired. □

Note that we had to use the full strength of the uniqueness of shortest primary decompositions to prove this statement.

We conclude this subsection with a characterization of the Noetherian domains which are normal.

Theorem 15.4.3. *Let A be a Noetherian domain. Then A is normal if and only if the following two statments hold:*

(a) *If P is a ht 1 prime ideal, then A_P is a DVR.*
(b) *If $a \neq 0$, every $P \in \mathrm{Ass}(A/(a))$ has ht 1.*

Proof. First assume A is normal. Then (a) holds, since A_P is a Noetherian local domain of dimension 1 which is normal, hence a DVR by Proposition 15.1.1. Also, Proposition 15.4.2 ensures that (b) holds.

Conversely, suppose (a) and (b) hold. By the proof of (ii) in Proposition 15.4.2, (b) implies that $A = \bigcap_{\mathrm{ht}(P)=1} A_P$. By (a), each A_P appearing in this intersection is normal, and thus A is normal too. □

16. Lecture 16

Beginning of completions. Basic questions arising for $\widehat{G}$. On exactness of $G \mapsto \widehat{G}$, and completeness of $\widehat{G}$.

16.1. **Completions of abelian topological groups.** Suppose $(G, +)$ is an abelian topological group. This means that G is an abelian group and also a topological space, such that the group operations $+ : G \times G \to G$ and $\mathrm{inv} : G \to G$ are continuous functions (where in the first case, $G \times G$ has the product topology).

Note that G is not necessarily Hausdorff. In fact, G is Hausdorff if and only if $\{0\}$ is a closed set. One direction is immediate: if G is Hausdorff, then any point is a closed set; in particular $\{0\}$ is closed. Conversely,, suppose $\{0\}$ is a closed set, and consider the continuous map

$$d : G \times G \to G$$

given by $d(x, y) = x - y$. Then clearly $d^{-1}\{0\} = \Delta \subset G \times G$, where Δ denotes the diagonal subset. So Δ is a closed subset, and it follows that G is Hausdorff. (In fact, a space X is Hausdorff iff the diagonal $\Delta \subset X \times X$ is closed.)

We define the **completion** $\widehat{G}$ to be the set of all equivalence classes of Cauchy sequences in G. Recall that a sequence $\{x_n\}$ is **Cauchy** if $x_n - x_m \to 0$ as $n, m \to \infty$ (I leave it to you to make this precise). Also, two Cauchy sequences $\{x_n\}$ and $\{y_n\}$ are **equivalent** provided that $x_n - y_n \to 0$ as $n \to \infty$.

Clearly, we may add or subtract Cauchy sequences term-by-term, and this gives well-defined operations of $+, -$ on $\widehat{G}$. It is easy to check that $\widehat{G}$ is itself an abelian group, and that the map $G \to \widehat{G}$ given by taking $g \in G$ to the "constant" Cauchy sequence $\{g\}$, is a group homomorphism.

Lemma 16.1.1. *G is Hausdorff if and only if $G \hookrightarrow \widehat{G}$.*

Proof. Let $H := \{0\}^-$, the closure of the subgroup $\{0\}$. Clearly H is a subgroup of G.
Claim: $\{0\}^- = \bigcap_{0 \in U} U$.
Proof:

$$x \in \bigcap_{0 \in U} U \Leftrightarrow 0 \in x - U, \forall U \ni 0$$
$$\Leftrightarrow x \in \{0\}^-,$$

the last equivalence holding because the open sets $x - U$ form a neighborhood basis of open sets containing x, as U varies over all open subsets containing 0.

Finally, $H = \ker(G \to \widehat{G})$. So we are done. □

Now we assume the topology on G is such that there is a countable sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n \supset \cdots$$

which form a basis of opens sets around $0 \in G$. This means that a subset $V \subset G$ is a neighborhood of 0 iff it contains contains some G_n. In particular, each G_n is an open and therefore a closed subgroup of G.

We have projections $\theta_{n+1} : G/G_{n+1} \to G/G_n$, so we can form the inverse limit

$$\varprojlim G/G_n \subset \prod G/G_n,$$

the subset of the direct product consisting of tuples $(x_n)_n \in \prod G/G_n$ such that for all $n \geq 0$, $\theta_{n+1}\, x_{n+1} = x_n$.

Unless otherwise mentioned, $\widehat{G}$ will denote the completion of G with respect to the topology determined by the filtration $G \supset \cdots \supset G_n \supset \cdots$.

Proposition 16.1.2. *There is a canonical isomorphism of abelian groups*

$$\widehat{G} = \varprojlim G/G_n.$$

Proof. If $\{\xi_n\}$ is a Cauchy sequence, then ξ_N is ultimately constant in G/G_n. So we can define a map $\widehat{G} \to \varprojlim G/G_n$ by sending $\{\xi_n\} \mapsto (x_n)_n$, where

$$x_n \equiv \xi_N \bmod G_n, \forall N >> 0.$$

To define the inverse map, let $\xi_n \in G$ be an arbitrary lift of $x_n \in G/G_n$. Then $\{\xi_n\}$ is a Cauchy sequence whose equivalence class is independent of the choice of lifts. □

Each G/G_n is a discrete abelian group, and the product topology on $\prod G/G_n$ makes the latter a topological abelian group. Then $\widehat{G} = \varprojlim G/G_n$ is also a topological abelian group (give it the subspace topology from $\prod G/G_n$).

Questions: In what sense is $G \mapsto \widehat{G}$ functorial? Is $\widehat{\widehat{G}} \cong \widehat{G}$? Does the topology on $\widehat{G}$ depend on the choice of subgroups G_n?

We shall answer these questions (at least for the concrete cases we need) in the next few sections.

16.2. **Functoriality of $G \mapsto \widehat{G}$.** So far, it is pretty obvious that $G \mapsto \widehat{G}$ gives us a functor $\underline{\text{Top.Ab}} \to \underline{\text{Ab}}$. In fact any continuous homomorphism $f : G_1 \to G_2$ determines a homomorphism $\widehat{f} : \widehat{G}_1 \to \widehat{G}_2$: if $\{\xi_n\} \subset G_1$ is Cauchy, then $\{f(\xi_n)\} \subset G_2$ is also Cauchy.

Exercise 16.2.1. *Assume that the topologies on G_1 and G_2 are defined by countable neighborhood bases of subgroups. Show that for the topologies on $\widehat{G}_1$ and $\widehat{G}_2$ defined above, the map $\widehat{f} : \widehat{G}_1 \to \widehat{G}_2$ just defined is continuous.*

Our next goal is to show that the functor $G \mapsto \widehat{G}$ is *exact*, in a certain sense. To state the proposition suppose we are given an exact sequence of topological abelian groups

$$0 \longrightarrow G' \longrightarrow G \xrightarrow{p} G'' \longrightarrow 0$$

where we are assuming G has topology given by the filtration G_n, $G' \subset G$ has the subspace topology (therefore has basis $G'_n := G' \cap G_n$ around 0) and G'' has the quotient topology (therefore has basis $G''_n := p(G_n)$ around 0).

Proposition 16.2.2 (Mittag-Leffler lemma)**.** *The sequence*

$$0 \longrightarrow \widehat{G'} \longrightarrow \widehat{G} \xrightarrow{p} \widehat{G''} \longrightarrow 0$$

is exact, where the completions $\widehat{G'}$ and $\widehat{G''}$ are defined using the filtrations G'_n and G''_n respectively.

Proof. It's ETS that

$$0 \longrightarrow \varprojlim G'/G'_n \longrightarrow \varprojlim G/G_n \xrightarrow{p} \varprojlim G''/G''_n \longrightarrow 0$$

is exact. More generally, suppose we have an exact sequence of inverse systems of abelian groups

$$0 \longrightarrow A_\bullet \longrightarrow B_\bullet \xrightarrow{p} C_\bullet \longrightarrow 0.$$

Then we will prove

(1)
$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \xrightarrow{p} \varprojlim C_n$$
is exact;

(2) the map $p : \varprojlim B_n \to \varprojlim C_n$ is surjective, if we assume $\theta_{n+1} : A_{n+1} \to A_n$ is surjective for all $n \geq 0$.

Let $A := \prod A_n$, and define $d^A : A \to A$ by $(a_n)_n \mapsto (a_n - \theta_{n+1} a_{n+1})_n$. Note that $\ker d^A = \varprojlim A_n$. Similarly define B, C, d^B, d^C. We have the commutative diagram with exact rows

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

The snake lemma gives the short exact sequence

$$0 \longrightarrow \ker d^A \longrightarrow \ker d^B \longrightarrow \ker d^C,$$

ie., statement (1).

For (2), again by the snake lemma it's ETS that coker $d^A = 0$, i.e that d^A is surjective. So, given $(a_n)_n \in A$, we must find $(a'_n)_n \in A$ such that

$$a_n = a'_n - \theta_{n+1} a'_{n+1},$$

for all $n \geq 0$. Since θ_{n+1} is surjective, we can solve for the a'_n's recursively. □

Corollary 16.2.3. *For all n, we have inclusions $\widehat{G}_n \hookrightarrow \widehat{G}$.*

Now we can define a topology on $\widehat{G}$ by declaring that the sequence of subgroups

$$\widehat{G} \supset \widehat{G}_1 \supset \widehat{G}_2 \supset \cdots$$

defines a basis of open subsets around $0 \in \widehat{G}$.

Exercise 16.2.4. *Show that this topology on $\widehat{G}$ agrees with the one defined by giving $\varprojlim G/G_n$ the subspace topology from the product $\prod G/G_n$.*

Proposition 16.2.5. *There is a canonical isomorphism $\widehat{G} \xrightarrow{\sim} \widehat{\widehat{G}}$. In particular, $\widehat{G}$ is Hausdorff and complete (every Cauchy sequence in $\widehat{G}$ converges).*

Proof. The exact sequence

$$0 \longrightarrow G_n \longrightarrow G \longrightarrow G/G_n \longrightarrow 0$$

gives us the exact sequence

$$0 \longrightarrow \widehat{G}_n \longrightarrow \widehat{G} \longrightarrow \widehat{G/G_n} \longrightarrow 0.$$

Since G/G_n is discrete, we have $\widehat{G/G_n} = G/G_n$, and hence a canonical isomorphism

$$G/G_n \xrightarrow{\sim} \widehat{G}/\widehat{G}_n.$$

So

$$\widehat{G} = \varprojlim G/G_n \xrightarrow{\sim} \varprojlim \widehat{G}/\widehat{G}_n = \widehat{\widehat{G}}.$$

□

16.3. **Examples: I-adic completions of rings and modules.** In the following examples, A denotes a ring with ideal $I \subset A$, and M is an A-module.

Examples

(a) Let $G = A$, $G_n = I^n$. Note that A is a topological ring WRT [5] the I-adic topology given by

$$A \supset I \supset I^2 \supset \cdots.$$

(b) Let $G = M$, $G_n = I^n M$. Then M is a topological A-module when both A and M are given the I-adic topologies. Furthermore $\widehat{A}$ is a topological ring, and $\widehat{M}$ is a topological $\widehat{A}$-module, i.e. the natural action map $\widehat{A} \times \widehat{M} \to \widehat{M}$ is continuous. This follows from the fact that $\widehat{A} \times I^n \widehat{M}$ is mapped by the action map into $I^n \widehat{M}$.

(c) M is Hausdorff for the I-adic topology iff $[\ker M \to \widehat{M}] = \cap_{n=1}^{\infty} I^n M = (0)$.

(d) If $f : M \to N$ is A-linear, it is automatically continuous for the I-adic topologies (check this!). Thus $M \mapsto \widehat{M}$ is a functor from A-modules to $\widehat{A}$-modules.

[5] With Respect To

(e) Letting $A = \mathbb{Z}$, and $I = (p)$, we get the p-adic ring $\widehat{A} = \mathbb{Z}_p$. Similarly, letting $A = k[X]$ and $I = (X)$, we get $\widehat{A} = k[[X]]$.

17. Lecture 17

Applications to I-adic completions of A and M. (Stable) I-filtrations, and proof of Artin-Rees lemma. Application: I-adic completion is an exact functor on category of f.g. modules over a Noeth. ring. More applications.

****

17.1. **Basic notions related to I-filtrations.** Let A be Noetherian, $I \subset A$ an ideal, and M a f.g. A-module.

Goal: If $0 \to M' \to M \to M'' \to 0$ is exact, then $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$ is exact, where each completion is defined using the I-adic topology.

N.B.: This does not follow immediately from Proposition 16.2.2: it is not at all obvious that the I-adic topology on M' is the subspace topology M' inherits from M. We need to prove this.

Theorem 17.1.1. *Let A, I, M be as above, and let $M' \subset M$ be a submodule. The the filtrations $I^n M'$ and $M' \cap I^n M$ have bounded difference, hence define the same topology on M' (and hence the same completion).*

Let us first recall some basic facts and terminology. We say $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ is an **I-filtration** if $IM_n \subset M_{n+1}$ for all $n \geq 0$. We say it is a **stable I-filtration** if also $IM_n = M_{n+1}$ for all $n >> 0$. For instance, $I^n M$ is a stable I-filtration.

Lemma 17.1.2. *Any stable I-filtrations M_n, M'_n have bounded difference: there exists n_0 such that $M_{n+n_0} \subset M'_n$ and $M'_{n+n_0} \subset M_n$ for all $n \geq 0$.*

Proof. WLOG $M'_n = I^n M$. Since M_n is an I-filtration, $I^n M \subset M_n$, $\forall n$, hence $I^{n+n_0} M \subset M_n$, $\forall n, n_0$.

Since M_n is stable, $\exists n_0$ such that $I^n M_{n_0} = M_{n+n_0}$, $\forall n$, hence $M_{n+n_0} = I^n M_{n_0} \subset I^n M$, $\forall n$. □

By the lemma, it's ETS that $M' \cap I^n M$ is a stable I-filtration on M'. We need to take a detour through graded rings/modules.

17.2. **Graded rings and modules.** Let $A = \oplus_{n=0}^{\infty} A_n$ be a **graded ring**: $A_0 \subset A$ is a subring, and $A_n A_m \subset A_{n+m}$, $\forall n, m$. In particular, $A_+ := \oplus_{n=1}^{\infty} A_n$ is an ideal in A.

Let $M = \oplus_{n=0}^{\infty} M_n$ be a **graded A-module**: $A_n M_m \subset M_{n+m}$, $\forall n, m$. In particular, each M_n is an A_0-module..

Let N also be a graded A-module. An A-module morphism $f : M \to N$ is **graded** if $f(M_n) \subset N_n$, $\forall n$.

Lemma 17.2.1. *TFAE:*

(1) *A is Noetherian.*
(2) *A_0 is Noetherian and A is a f.g. A_0-algebra.*

Proof. (2) ⇒ (1): Use Hilbert's Basis Theorem.

(1) ⇒ (2): $A_0 = A/A_+$, hence is Noetherian. The ideal A_+ is f.g.. Suppose $A_+ = (y_1, \ldots, y_r)$, where WLOG $y_i \in A_{k_i}$, for $k_i > 0$. Let $A' := A_0[y_1, \ldots, y_r]$. We will prove that $A' = A$; it's ETS that $A_n \subset A'$ for all n, which we prove by

induction on n. If $y \in A_n$, write $y = \sum_i a_i y_i$ for some $a_i \in A_{n-k_i}$ (take $a_i = 0$ if $n < k_i$). We are done because the induction hypothesis gives $a_i \in A'$ for all i. $\square$

Now let A be a ring, and let M be an A-module equipped with an I-stable filtration M_n. We will apply the above considerations to the graded ring $A^* := \oplus_{n=0}^{\infty} I^n$ and its graded module $M^* := \oplus_{n=0}^{\infty} M_n$. (Check that these are indeed graded rings/modules.)

Lemma 17.2.2. *With the notation above, assume A is Noetherian and M is f.g. Then TFAE:*

(i) *M^* is a f.g. A^*-module.*
(ii) *M_n is stable.*

Proof. Since M_n is a f.g. A-module, so is $Q_n := \oplus_{r=0}^{n} M_r \subset M^*$. It is easy to see (check this!) that Q_n generates the A^*-submodule

$$M_n^* := M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots .$$

Note that M_n^* is f.g. as an A^*-module (since Q_n is f.g. as an A-module). Since A^* is Noetherian (Lemma 17.2.1), M^* is f.g. as an A^*-module iff the following ascending chain which exhausts M^* is stationary:

$$M_n^* \subset M_{n+1}^* \subset \cdots ,$$

which holds iff

$$\begin{aligned} M^* = M_n^* \text{ for some } n &\Leftrightarrow M_{n+n_0} = I^n M_{n_0}, \text{ for some } n_0 \text{ and every } n \\ &\Leftrightarrow M_n \text{ is stable.} \end{aligned}$$

$\square$

This gives us the next very useful result.

Proposition 17.2.3 (Artin-Rees Lemma)**.** *Suppose A is Noetherian, $I \subset A$ is an ideal, M is a f.g. A-module, M_n is a stable I-filtration in M, and $M' \subset M$ is a submodule. Then $M' \cap M_n$ is a stable I-filtration on M'.*

Proof. We have $I(M' \cap M_n) \subset M' \cap IM_n \subset M' \cap M_{n+1}$, so $M' \cap M_n$ is an I-filtration. Applying Lemma 17.2.2 to both M^* and $\oplus_n M' \cap M_n$, we see first that M^* is a f.g. A^*-module, and further that

$$\begin{aligned} \oplus_n M' \cap M_n \text{ is a graded } A^*\text{-submodule of } M^* &\Rightarrow \text{it is a f.g. } A^*\text{-module} \\ &\Rightarrow M' \cap M_n \text{ is stable.} \end{aligned}$$

$\square$

17.3. **Some consequences of Artin-Rees.** There is an obvious map $\widehat{A} \otimes_A M \to \widehat{M}$ (here completions are the I-adic ones).

Proposition 17.3.1. (1) *If M is f.g, then $\widehat{A} \otimes_A M \twoheadrightarrow \widehat{M}$.*
(2) *If A is Noetherian and M is f.g., then $\widehat{A} \otimes_A M \xrightarrow{\sim} \widehat{M}$.*

Proof. (1): There is an exact sequence $0 \to N \to A^n \to M \to 0$. This gives a commutative diagram with exact upper row

$$\begin{array}{ccccccccc} & & \widehat{A} \otimes_A M & \longrightarrow & \widehat{A}^n & \longrightarrow & \widehat{A} \otimes_A M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \cong & & \downarrow & & \\ 0 & \longrightarrow & \widehat{N} & \longrightarrow & \widehat{(A^n)} & \xrightarrow{\delta} & \widehat{M} & \longrightarrow & 0. \end{array}$$

(We could have asserted that the bottom row is also exact, had we assumed A Noetherian; in any case the map δ is surjective, by the Mittag-Leffler lemma.) Now it follows that the right vertical map is surjective, and (1) holds.
(2): If A is Noetherian, then the bottom row is exact, and N is f.g., so we have the surjectivity of the left vertical arrow from part (1). But now the snake lemma implies that the right vertical arrow is an isomorphism. □

Corollary 17.3.2. *If A is Noetherian, then any I-adic completion $\widehat{A}$ is a flat A-module.*

Proof. The implication $M' \hookrightarrow M \Rightarrow \widehat{A} \otimes_A M' \hookrightarrow \widehat{A} \otimes_A M$ holds when M', M are f.g. modules, by the left-exactness of the functor $\widehat{\cdot}$ on f.g. modules. But this is sufficient to prove this implication for arbitrary M', M, by Atiyah-Macdonald, Prop. 2.19. □

18. Lecture 18

Further consequences of Artin-Rees, such as Krull's theorem. Associated graded rings/modules. Proof that A Noeth $\Rightarrow \widehat{A}$ Noeth. Geom. meaning of $G(A)$: "tangent cone". Hensel's lemma.
****

18.1. **Further consuequences of Artin-Rees.**

Lemma 18.1.1. *Suppose A is Noetherian, $I \subset A$ is an ideal, and $\widehat{\cdot}$ denotes I-adic completion.*

(0) *If M is a f.g. A-module, and $M' \subset M$ is a submodule, then $\exists k \in \mathbb{Z}_{\geq 0}$ such that $I^{n-k}(I^k M \cap M') = I^n M \cap M'$, for all $n \geq k$.*
(1) $\widehat{I} = \widehat{A}I \cong \widehat{A} \otimes_A I$.
(2) $\widehat{I^n} = \widehat{I}^n$.
(3) $I^n/I^{n+1} \cong \widehat{I}^n/\widehat{I}^{n+1}$. *Similarly,* $A/I^n = \widehat{A}/\widehat{I}^n$.
(4) $\widehat{I} \subset$ *Jac. rad. of* $\widehat{A}$.

Proof. (0): This is a reformulation of the fact that $I^n M \cap M'$ is a stable I-filtration on M', a consequence of the Artin-Rees lemma.
(1): We have established the natural isomorphism $\widehat{A} \otimes_A I \xrightarrow{\sim} \widehat{I}$. Note that the image of this map is just $\widehat{A}I$.
(2): By (1), we have $\widehat{I^n} = \widehat{A}I^n = (\widehat{A}I)^n = \widehat{I}^n$.
(3): By (2) and exactness of $\widehat{\cdot}$, we have $\widehat{I}^n/\widehat{I}^{n+1} = \widehat{I^n}/\widehat{I^{n+1}} = \widehat{I^n/I^{n+1}}$. This is just I^n/I^{n+1}, since the latter is discrete.
(4): Note that since $\widehat{I}^n = \widehat{I^n}$, the ring $\widehat{A}$ is complete for the $\widehat{I}$-adic topology. But then for any $\alpha \in \widehat{I}$, we have the convergent geometric series

$$(1-\alpha)^{-1} = 1 + \alpha + \alpha^2 + \cdots \in \widehat{A},$$

and so $1-\alpha \in \widehat{A}^\times$. It follows that α belongs to the Jacobson radical of $\widehat{A}$. $\square$

Lemma 18.1.2. *If $(A,\mathfrak{m})$ is a Noetherian local ring, and $\widehat{A}$ is the $\mathfrak{m}$-adic completion, the $(\widehat{A},\widehat{\mathfrak{m}})$ is local.*

Proof. By (3), $\widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}$, and so $\mathfrak{m}$ is a maximal ideal in $\widehat{A}$. By (4), $\mathfrak{m}$ is the Jacobson radical, and hence is the only maximal ideal. $\square$

Theorem 18.1.3 (Krull's Theorem)**.** *Suppose A is Noetherian, $I \subset A$ is an ideal, M is a f.g. A-module, and $\widehat{M}$ is its I-adic completion. Let $E := \cap_{n=0}^\infty I^n M$, the kernel of the natural map $M \to \widehat{M}$. Then*

$$E = \{x \in M \mid (1-\alpha)x = 0 \text{ for some } \alpha \in I\}.$$

Proof. Note that the subspace topology E inherits from M is the trivial one: the only open subsets are $\emptyset$ and E itself. By the Artin-Rees lemma, the I-adic topology on E is also trivial, which means that $E = IE$. If $E = Ax_1 + \cdots + Ax_n$, then we may write $x_i = \sum_j \alpha_{ij} x_j$, for some $\alpha_{ij} \in I$. Then the element $\det(\alpha_{ij} - \delta_{ij}) \in \pm 1 + I$ kills E (by the "Cramer's Rule Trick").

Conversely, $(1-\alpha)x = 0$, $\alpha \in I \implies x = \alpha x = \alpha^2 x = \cdots \in \cap_{n=1}^\infty I^n M = E$. $\square$

Corollary 18.1.4. *If A is a Noetherian domain, and $I \neq (1)$, then $\cap_{n=1}^\infty I^n = 0$.*

Proof. Note that $1+I$ has no zero-divisors. $\square$

Corollary 18.1.5. *If A is Noetherian and the ideal I belongs to the Jacobson radical of A, and M is a f.g. A-module, then $\cap_{n=1}^\infty I^n M = 0$ (and thus M is Hausdorff WRT the I-adic topology). In particular, if $(A,\mathfrak{m})$ is Noetherian local, and M is f.g., then $\cap_{n=1}^\infty \mathfrak{m}^n M = 0$.*

Proof. Note that $1 + I \subset A^\times$. $\square$

Corollary 18.1.6. *If B is Noetherian, and $\mathfrak{p} \in \mathrm{Spec}(B)$, then $\ker(B \to B_\mathfrak{p})$ is the intersection of the $\mathfrak{p}$-primary ideals of B.*

Proof. See Atiyah-Macdonald, 10.21. $\square$

18.2. *A* **Noetherian implies $\widehat{A}$ Noetherian.** Our goal is to prove that $\widehat{A}$ is Noetherian if A is. We need to study associated graded rings/modules.

Suppose I is an ideal in a ring A, and M is an A-module equipped with an I-filtration M_n. Define the **associated graded ring** $G_I(A) := \oplus_{n=0}^\infty I^n/I^{n+1}$. Similarly, define the **associated graded module** $G_I(M) := \oplus_{n=0}^\infty M_n/M_{n+1}$.

It is clear that $G_I(A)$ is a graded ring, with multiplication defined by $\overline{x_n} \cdot \overline{x_m} = \overline{x_n x_m}$ (where this notation has the obvious meaning). Also, $G_I(M)$ is a graded module over $G_I(A)$.

Proposition 18.2.1. *Suppose A is Noetherian.*

1. *$G_I(A)$ is Noetherian.*
2. *$G_{\widehat{I}}(\widehat{A}) = G_I(A)$.*
3. *If M is a f.g. A-module, and M_n is stable, then $G(M)$ is f.g. $G(A)$-module.*

Proof. (1): Write $I = (x_1, \ldots, x_r)$, and $I/I^2 = (\bar{x}_1, \ldots, \bar{x}_r)$. Then $G(A) = A/I[\bar{x}_1, \ldots, \bar{x}_r]$, hence is Noetherian by the Hilbert basis theorem.
(2): This is clear from Lemma 18.1.1.
(3): Suppose $M_{n_0+n} = I^n M_{n_0}$ for $n \geq 0$. Then $G(M)$ is generated over $G(A)$ by $\oplus_{n=0}^{n_0} M_n/M_{n+1}$. Each M_n/M_{n+1} is f.g. as an A/I-module, hence we are done. $\square$

We need a kind of converse to the implication in (3) above. The following lemma is a crucial tool.

Lemma 18.2.2. *Suppose $\phi : A \to B$ is a homomorphism of filtered abelian groups, i.e., $\phi(A_n) \subset B_n$ for all n. Clearly ϕ induces maps $G(\phi) : G(A) \to G(B)$ and $\widehat{\phi} : \widehat{A} \to \widehat{B}$. Then:*

(1) *$G(\phi)$ injective $\implies$ $\widehat{\phi}$ is injective.*
(2) *$G(\phi)$ surjective $\implies$ $\widehat{\phi}$ is surjective.*

Proof. See Atiyah-Macdonald, 10.23. □

Lemma 18.2.3. *Suppose A is I-adically complete, and M has a separated I-filtration M_n (i.e. $\cap_n M_n = 0$). Then $G(M)$ f.g. over $G(A)$ $\implies$ M is f.g. over A.*

Proof. Choose a finite set of homogeneous generators $x_i \in M_{n(i)}$ for $G(M)$ over $G(A)$. Define $F^i = A$ endowed with the stable I-filtration $F^i_k := I^{k-n(i)}$ (where we set $I^\nu = A$ if $\nu < 0$). Define

$$\phi : F := \oplus_i F^i \to M$$

by $e_i \mapsto x_i \in M_{n(i)}$, where e_i is the ith standard basis vector. This map is filtered in the sense of the previous lemma. By definition $G(\phi)$ is surjective, and so by Lemma 18.2.2, $\widehat{\phi}$ is surjective. Now consider the commutative diagram

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ \cong\downarrow & & \downarrow \\ \widehat{F} & \xrightarrow{\widehat{\phi}} & \widehat{M}. \end{array}$$

The left vertical arrow is an isomorphism because $A = \widehat{A}$. Since $\widehat{\phi}$ is surjective, we see that the right vertical arrow is surjective. But then the right vertical arrow is an isomorphism (it is injective since $\cap_n M_n = 0$). Now going around the diagram, we see that ϕ is surjective, and so M is f.g. as an A-module. □

Corollary 18.2.4. *Let A, M be as above. Then $G(M)$ is a Noetherian $G(A)$-module $\implies$ M is a Noetherian A-module.*

Proof. Let $M' \subset M$ be a submodule; we want to show M' is f.g. as an A-module. Consider the separated I-filtration $M'_n := M' \cap M_n$. We have $M'_n/M'_{n+1} \hookrightarrow M_n/M_{n+1}$, which implies that $G(\phi) : G(M') \hookrightarrow G(M)$. Thus $G(M')$ is a f.g. $G(A)$-module, and then by Lemma 18.2.3, we see M' if a f.g. A-module. □

Theorem 18.2.5. *A Noetherian $\implies$ $\widehat{A}$ Noetherian.*

Proof. Note that $G_I(A) = G_{\widehat{I}}(\widehat{A})$ so the latter is Noetherian. Also, $\widehat{A}$ is $\widehat{I}$-adically complete (Lemma 18.1.1), and so the $\widehat{I}$-adic topology is separated: $\cap_n \widehat{I}^n = 0$. Applying the above corollary to $M = \widehat{A}$, we get that $\widehat{A}$ is Noetherian. □

Remark 18.2.6.

- *If k is a field, then $k[[X_1, \ldots, X_n]]$ is Noetherian, since it is the $(X_1, \ldots, X_n)$-adic completion of the Noetherian ring $k[X_1, \ldots, X_n]$.*
- *Let $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$. Then the following two $\mathfrak{m}$-adic completions are canonically isomorphic: $\widehat{A} = \widehat{A_{\mathfrak{m}}}$. Why? Use the identities $A_{\mathfrak{m}}/\mathfrak{m}^n A_{\mathfrak{m}} = (A/\mathfrak{m}^n)_{\mathfrak{m}} = A/\mathfrak{m}^n$.*

18.3. **Geometric meaning of the associated graded ring: the tangent cone.** The following discussion is taken from Mumford's book *The Red Book of Varieties and Schemes*, III, §3. Suppose $k = \overline{k}$. Given a closed point $x \in V(I)$ for $I \subset k[X_1, \dots, X_n]$ a radical ideal, let $A = k[X_1, \dots, X_n]/I$ and let $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(A)$ be the maximal ideal corresponding to x. Then we define the *tangent cone to* $V(I)$ *at* x to be the affine scheme $\mathrm{Spec}(G_{\mathfrak{m}}(A))$.

How can we "compute" this scheme? Mumford explains it, and here we just give the answer: WLOG x is the origin in the ambient affine space $\mathbb{A}^n$. For any element $0 \neq f \in k[X_1, \dots, X_n]$, write it in the form $f = f_s + f_{s+1} + \cdots + f_{s+r}$, where $f_s \neq 0$ and each summand f_k is the degree k homogeneous part of f; denote the lowest degree term f_s simply by f^*. Let I^* be the ideal generated by all f^*, where f ranges over all elements $0 \neq f \in I$. Then

$$G_{\mathfrak{m}}(A) = k[X_1, \dots, X_n]/I^*.$$

From this, we can see why $\mathrm{Spec}(G_{\mathfrak{m}}(A))$ is called the tangent cone. Let's consider two examples:

Curve with cusp: Let $V(I)$ be the plane curve given by $Y^2 - X^3$. Then $f^* = Y^2$, and so the tangent cone at $(0,0) \in V(I)$ is the spectrum of the ring $k[X,Y]/Y^2$, in other words, the "X-axis with multiplicity two". Note that the tangent cone is an affine scheme but is not an affine variety (the ring is not reduced), even though the curve we started out with was a variety. This is another example of how schemes enter into the study of varieties.

Nodal curve: Let $V(I)$ be the place curve given by $X^2 - Y^2 + X^3$. Then $f^* = (X - Y)(X + Y)$, and the tangent cone at $(0,0)$ is the union of the lines $X = \pm Y$.

18.4. **Hensel's Lemma.** This is another application of complete local rings. For motivation, consider the equation $X^2 + 1 = 0$ in $\mathbb{Z}[X]$. It has no solutions $X \in \mathbb{Z}$. However, modulo 5, this equation has two distinct solutions, namely, $\overline{X} = 2, 3$. We can't lift these solutions to $\mathbb{Z}$, but we *can* lift them to the completion of $\mathbb{Z}$ at the prime ideal $5\mathbb{Z}$, namely the 5-adic numbers $\mathbb{Z}_5$. Indeed that is a very special case of the following result.

Proposition 18.4.1 (Hensel's Lemma)**.** *Let $(A, \mathfrak{m})$ be a local ring such that A is $\mathfrak{m}$-adically complete. Let $k := A/\mathfrak{m}$. Suppose $F(X) \in A[X]$ is monic, and write $\overline{F}(X) \in k[X]$ for its reduction modulo $\mathfrak{m}$. If $\overline{F} = gh$ in $k[X]$, where $(g,h) = 1$ and g, h are monic, then there exist monic $G, H \in A[X]$ such that $F = GH$ and $\overline{G} = g$, $\overline{H} = h$.*

Proof. Choose arbitrary monics $G_1, H_1 \in A[X]$ which lift g, h respectively. Then $F \equiv G_1 H_1 \bmod \mathfrak{m}[X]$.

By induction, suppose we have constructed monics $G_n, H_n \in A[X]$ with $\overline{G_n} = g$, $\overline{H_n} = h$, and $F \equiv G_n H_n \bmod \mathfrak{m}^n[X]$. Then we can write

$$F - G_n H_n = \sum_i \omega_i U_i(X)$$

where $\omega_i \in \mathfrak{m}^n$ and $\deg(U_i) < \deg(F)$, for all i.

Since $(g,h) = 1$, there exist $v_i, w_i \in k[X]$ such that $\overline{U_i} = gv_i + hw_i$. WLOG $\deg(v_i) < \deg(h)$ (if necessary, replace v_i with its remainder mod h, absorbing the difference into w_i).

Then $\deg(hw_i) = \deg(\overline{U_i} - gv_i) < \deg(F)$, hence $\deg(w_i) < \deg(g)$.

Choose $V_i, W_i \in A[X]$ such that $\overline{V_i} = v_i, \overline{W_i} = w_i$, and with $\deg(V_i) = \deg(v_i)$ and $\deg(W_i) = \deg(w_i)$. Set

$$G_{n+1} = G_n + \sum_i \omega_i W_i$$
$$H_{n+1} = H_n + \sum_i \omega_i V_i.$$

Note that $F \equiv G_{n+1}H_{n+1} \bmod \mathfrak{m}^{n+1}[X]$ (check this!). We then set

$$\lim_{n\to\infty} G_n = G$$
$$\lim_{n\to\infty} H_n = H.$$

(By construction and the completeness of A, these limits exist.) It is easy to check that G, H have the desired properties. □

19. Lecture 19

Hilbert functions, etc: Motivation comparing $\dim A_0[X_1, \ldots, X_s] = s$ with $\mathrm{ord}_{t=1}P(A,t)$ and $\deg_n \ell_{A_0} A_n$...

Rationality and explicit expression for $P(M,t)$. Lemma for I-stable filt M_n of graded A-module M: $\ell(M/M_n) = g(n)$ for $n >> 0$.

****

19.1. **Combinatorics and a motivating example.** We consider the polynomial ring $A = A_0[X_1, \ldots, X_s]$, where A_0 is an Artin ring (that is, a Noetherian ring of dimension 0). This is a graded ring $A = \oplus_{n\geq 0} A_n$, where A_n is the free A_0-module generated by the set of monomials of form $X_1^{m_1} \cdots X_s^{m_s}$, where $m_i \geq 0$ and $\sum_i m_i = n$. It is not hard to count these monomials: arrange $n + s - 1$ dots in a row, and cross out $s - 1$ of them. We get s ordered clumps of dots, with say m_i dots in the ith clump, and the total number of remaining dots is n. Clearly such arrangements correspond bijectively to the monomials we are counting. On the other hand, the number of possible such arrangements is simply $\binom{n+s-1}{s-1}$.

As a consequence, setting all X_i to t in the obvious formula

$$\prod_{i=1}^{s}(1 - X_i)^{-1} = \sum_{n\geq 0}\Big(\sum_{|\underline{m}|=n} X_1^{m_1} \cdots X_s^{m_s}\Big) \tag{19.1.1}$$

yields

$$(1-t)^{-s} = \sum_{n\geq 0}\binom{n+s-1}{s-1}t^n = \sum_{n\geq 0}\mathrm{rank}_{A_0}(A_n)t^n, \tag{19.1.2}$$

where $\mathrm{rank}_{A_0}(A_n)$ denotes the rank of the A_0-module A_n. We have

$$\mathrm{rank}_{A_0}(A_n) = \ell_{A_0}(A_n) \cdot \ell_{A_0}(A_0)^{-1},$$

where $\ell_{A_0}(A_n)$ denotes the length of the A_0-module A_n.

We will see later that $\dim A = s + \dim A_0 = s$ (we already know this when A_0 is a field) [6]. Thus, we see that the dimension of A, which is s, is also the order of

[6] Actually, we won't have time for this. Here are the basic facts. If A is any ring and $B = A[X]$, then $\dim A + 1 \leq \dim B \leq 2\dim A + 1$. If A is Noetherian, then $\dim A + 1 = \dim B$. A good reference for this is [Serre], III.D.1.

the pole at $t = 1$ in the power series $\sum_{n\geq 0} \ell_{A_0}(A_n)t^n$. We will generalize this fact to other rings in the next sections.

19.2. **Hilbert functions.** Let $A = \oplus_n A_n$ be a Noetherian graded ring (so that A_0 is Noetherian, and there is a finite set of homogeneous elements $x_i \in A_{k_i}$, $k_i > 0$, such that $A = A_0[x_1, \ldots, x_s]$). Let $M = \oplus_n M_n$ be a f.g. graded A-module (so that each M_n is a f.g. A_0-module: indeed, if M is generated over A by homogeneous $m_1, \ldots, m_t$ of degree $r_1, \ldots, r_t$, then M_n is generated over A_0 by terms $g(x_1, \ldots, x_s)m_j$ where $r_j \leq n$ and g is a monomial of degree $n - r_j$).

Let λ be a $\mathbb{Z}$-valued additive function on the category of finite-length A_0-modules. This means that for a short exact sequence of such A_0-modules

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

we have $\lambda(M) = \lambda(M') + \lambda(M'')$. It follows that if $0 \to K_0 \to K_1 \to \cdots \to K_l \to 0$ is exact in this category, then $\sum_i (-1)^i \lambda(K_i) = 0$.

We define the **Poincare series** of M (WRT λ) to be the formal power series

$$P(M, t) := \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[[t]].$$

Theorem 19.2.1. *We have* $P(M, t) = \dfrac{f(t)}{\prod_{i=1}^{s}(1 - t^{k_i})}$, *for some* $f(t) \in \mathbb{Z}[t]$.

Proof. Induction on s. If $s = 0$, then $A = A_0$ and $M_n = 0$ for $n >> 0$. Thus $P(M, t) \in \mathbb{Z}[t]$ in this case.

Assume the theorem holds for graded rings generated over A_0 by $s-1$ elements. We have an exact sequence for every n

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0. \tag{19.2.1}$$

Let $K := \oplus_n K_n$ and $L := \oplus_n L_n$ (for the latter, the initial terms for $n < k_s$ are not defined – simply set them equal to 0). These are f.g. graded A-modules, killed by x_s (check!), so are f.g. graded $A_0[x_1, \ldots, x_{s-1}]$-modules.

Multiplying

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s})$$

by t^{k_s} and summing over n, we get the equality

$$(1 - t^{k_s})P(M, t) = -t^{k_s}P(K, t) + P(L, t) + g(t),$$

for some $g(t) \in \mathbb{Z}[t]$. Using the induction hypothesis applied to K, L, the result follows. □

Now we define

$$d(M) := \mathrm{ord}_{t=1} P(M, t),$$

the order of the pole at $t = 1$. The number $d(M)$ is an integer $\leq s$.

Corollary 19.2.2. *If* $k_i = 1$ *for all* i, *then* $\lambda(M_n)$, *as a function of* n, *belongs to* $\mathbb{Q}[n]$ *for sufficiently large* n, *having degree* $d(M) - 1$.

Proof. Let $d := d(M)$. WLOG $P(M, t) = \frac{f(t)}{(1-t)^d}$, where $f(1) \neq 0$. Write $f(t) = \sum_{k=0}^{N} a_k t^k$. Now $\lambda(M_n)$ is the coefficient of t^n in the product

$$\sum_{k=0}^{N} a_k t^k \cdot (1 - t)^{-d},$$

which by using (19.1.2) with $s = d$ is

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{n-k+d-1}{d-1}$$

as long as $n \geq N$. Viewed as a polynomial in n (with $\mathbb{Q}$-coefficients), this has leading term

$$(\sum_{k=0}^{N} a_k) n^{d-1}/(d-1)!,$$

proving the corollary. □

The following related result is also useful.

Proposition 19.2.3. *Suppose $x \in A_k$ is not a zero-divisor for M. Then $d(M/xM) = d(M) - 1$.*

Proof. In (19.2.1) we have $K_n = 0$, and the exact sequence becomes

$$0 \longrightarrow M_n \xrightarrow{x} M_{n+k} \longrightarrow L_{n+k} \longrightarrow 0.$$

From the previous argument, we see that $(1-t^k)P(M,t) = P(M/xM,t) + g(t)$ (for some polynomial g) and this implies the result. □

Proposition 19.2.4. *Let $(A, \mathfrak{m})$ be a Noetherian local ring, and I an $\mathfrak{m}$-primary ideal. Let M be a f.g. A-module, with a stable I-filtration M_n. Then*

(i) *$\ell_A(M/M_n) < \infty$.*
(ii) *If I is generated by s elements $x_1, \ldots, x_s$, then $\ell(M/M_n) = g(n)$ for $n >> 0$, where $g \in \mathbb{Q}[n]$ is a polynomial in n with degree $\leq s$.*
(iii) *The degree and leading coefficient of $g(n)$ depend on M and I, but not the choice of I-stable filtration M_n.*

Proof. (i): It's ETS $\ell(M_n/M_{n+1}) < \infty$. Now M_n/M_{n+1} is a f.g. A/I-module, and as A/I is Artin (being Noetherian and dim 0 – check this, using that I is $\mathfrak{m}$-primary), this means that $\ell(M_n/M_{n+1}) = \ell_{A/I}(M_n/M_{n+1}) < \infty$.
(ii): The associated graded ring $G(A) = A/I[x_1, \ldots, x_s]$ is Noetherian, and $G(M) = \oplus_n M_n/M_{n+1}$ is f.g. as a $G(A)$-module (since the filtration is stable). Therefore, by Corollary 19.2.2, $\ell(M_n/M_{n+1}) = f(n)$ is a polynomial in $\mathbb{Q}[n]$ for $n \geq n_0$ (some n_0), having degree $\leq s-1$. Now the equality

$$\ell(M/M_{n+1}) = \ell(M/M_{n_0}) + \ell(M_{n_0}/M_{n_0+1}) + \cdots + \ell(M_{n-1}/M_n) + \ell(M_n/M_{n+1}),$$

shows that for $n \geq n_0$, $\ell(M/M_n)$ is given by a polynomial $g(n) \in \mathbb{Q}[n]$ having degree $\leq s$.
(iii): Let $\widetilde{M_n}$ denote another I-stable filtration on M, and $\widetilde{g}(n) \in \mathbb{Q}[n]$ be the corresponding polynomial giving $\ell(M/\widetilde{M_n})$ for $n >> 0$. Since M_n and $\widetilde{M_n}$ have bounded difference, $\exists n_0$ such that $M_{n+n_0} \subset \widetilde{M_n}$ and $\widetilde{M}_{n+n_0} \subset M_n$ for all $n \geq 0$. It follows that $g(n+n_0) \geq \widetilde{g}(n)$ and $\widetilde{g}(n+n_0) \geq g(n)$ for all $n >> 0$ This implies that g and $\widetilde{g}$ have the same degree and leading coefficient. □

19.3. **Characteristic polynomial of a primary ideal.** We define $\chi_I^M(n) := g(n) = \ell(M/M_n)$. In the special case $M = A$, we call $\chi_I(n) := \chi_I^A(n)$ the **characteristic polynomial** of the $\mathfrak{m}$-primary ideal I.

Lemma 19.3.1. *Let $(A, \mathfrak{m}), I$ be as above. Then* $\deg \chi_I(n) = \deg \chi_{\mathfrak{m}}(n)$*, so that* $\deg \chi_I(n)$ *is independent of the choice of I.*

Proof. There exists an integer $r \geq 1$ such that $\mathfrak{m} \supset I \supset \mathfrak{m}^r$, so that $\mathfrak{m}^n \supset I^n \supset \mathfrak{m}^{rn}$, for all $n \geq 0$.

This implies that $\chi_{\mathfrak{m}}(n) \leq \chi_I(n) \leq \chi_{\mathfrak{m}}(rn)$ for all $n \geq 0$, which implies the result. □

Thus we may define the quantity $d(A) := \deg \chi_I(n)$, where I is any $\mathfrak{m}$-primary ideal. Note that

$$d(A) = d(G_{\mathfrak{m}}(A)),$$

where the RHS is defined as in the beginning of this section. From Corollary 19.2.2 and the equality

$$\deg_n \ell(A/\mathfrak{m}^n) = \deg_n \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) + 1$$

we see that $d(A) = d(G_{\mathfrak{m}}(A))$.

20. Lecture 20

Proof that $d(A) = \dim(A) = \delta(A)$, for Noetherian local rings A.
****

20.1. **The equality of three characterizations of Krull dimension.** Let $(A, \mathfrak{m})$ be a Noetherian local ring. We have not yet shown that the dimension of A is finite. We will next prove the stronger fact that the following three numbers are equal:

- $\dim A$
- $\delta(A) :=$ the minimal number of generators of an $\mathfrak{m}$-primary ideal
- $d(A) = \deg_n \chi_I(n)$, for any $\mathfrak{m}$-primary ideal I.

We'll show that $\delta(A) \geq d(A) \geq \dim A \geq \delta(A)$. We have already proved $\delta(A) \geq d(A)$. Indeed, this follows from Proposition 19.2.4, (ii).

Next, we will show $d(A) \geq \dim A$, by induction on $d(A)$. If $d(A) = 0$ then $\ell(A/\mathfrak{m}^n)$ is constant for large n, and hence $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for large n. By NAK this implies that $\mathfrak{m}^n = 0$ and so $A \cong A/\mathfrak{m}^n$. Thus A is Artin, and so $\dim A = 0$.

Now assume that $d(A) \geq 1$, and that the inequality holds for rings A' with $d(A') < d(A)$.

Claim: $\dim A \geq 1$.

Proof: If $\dim A = 0$, then $\mathfrak{m}$ is the unique prime ideal, and so (0) is $\mathfrak{m}$-primary. So using Lemma 19.3.1 we see $\chi_I(n)$ is constant and $d(A) = 0$, a contradiction.

Now write $r \geq 1$ for $\dim A$. Choose a chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in A.

Claim: $r \leq d(A)$.

Proof: Choose $x \in \mathfrak{p}_1$, $x \notin \mathfrak{p}_0$. Let $x' = \overline{x} \in A/\mathfrak{p}_0 =: A'$.

Note that $d(A') \leq d(A)$: $\mathfrak{m}' := \overline{\mathfrak{m}} \subset A'$ is maximal, and $A/\mathfrak{m}^n \twoheadrightarrow A'/(\mathfrak{m}')^n$. This implies $\ell(A'/(\mathfrak{m}')^n) \leq \ell(A/\mathfrak{m}^n)$, and so $d(A') \leq d(A)$.

Using this together with Lemma 20.1.1 below (applied to $B = A'$ and $y = x'$), we see $d(A'/(x')) \leq d(A') - 1 \leq d(A) - 1$, and hence the induction hypothesis applies to the ring $A'/(x')$. Thus $\dim A'/(x') \leq d(A'/(x'))$.

But modulo (x'), we have the chain $\overline{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \overline{\mathfrak{p}}_r$ in $\mathrm{Spec}(A'/(x'))$, and so the above remarks give us $r-1 \leq d(A)-1$, or $\dim A \leq d(A)$, as desired. The claim is proved, modulo the lemma below.

Lemma 20.1.1. *Let $(B,\mathfrak{n})$ be a Noetherian local ring with $\mathfrak{n}$-primary ideal I, and let M be a f.g. B-module. If $y \in B$ is not a zero-divisor in M, and if $\overline{M} := M/yM$, then* $\deg \chi_I^{\overline{M}} \leq \deg \chi_I^M - 1$. *In particular, taking $M = B$, we have $d(B/yB) \leq d(B)-1$.*

Proof. We have $N := yM \cong M$ as a B-module. Consider the exact sequence

$$0 \to N/(N \cap I^n M) \to M/I^n M \to \overline{M}/I^n\overline{M} \to 0.$$

We have

$$\ell(M/I^nM) = \ell(N/(N \cap I^n M)) + \ell(\overline{M}/I^n\overline{M}).$$

By Artin-Rees and $N \cong M$ (and using Proposition 19.2.4, (iii)), the first summand on the RHS has the same degree and leading coefficient as the LHS. This implies the desired bound on the degree of the remaining term on the RHS. □

It remains to prove the $\dim A \geq \delta(A)$. Write $d = \dim A$. It's enough to construct a sequence of elements

$$x_1, \ldots, x_i, \ldots, x_d$$

such that for each i the following holds:

(20.1.1) For any prime $\mathfrak{p} \supset (x_1, \ldots, x_i)$, we have $\mathrm{ht}(\mathfrak{p}) \geq i$.

Indeed, then for any prime $\mathfrak{p} \supset (x_1, \ldots, x_d)$ we would have $\mathrm{ht}(\mathfrak{p}) \geq d$, which can only happen if $\mathfrak{p} = \mathfrak{m}$. Thus $(x_1, \ldots, x_d)$ is $\mathfrak{m}$-primary, and is generated by d elements. Thus, $d \geq \delta(A)$.

We will construct the sequence $x_1, \ldots, x_d$ as in (20.1.1) by induction. Suppose $i \geq 1$ and we have already constructed $x_1, \ldots, x_{i-1}$ satisfying (20.1.1). Let $\mathfrak{p}_j$, for $j = 1, \ldots, l$, be the minimal primes containing $(x_1, \ldots, x_{i-1})$ having height $i-1$ (there might be no such primes).
Claim: $\mathfrak{m} \nsubseteq \cup_{j=1}^l \mathfrak{p}_j$.
Proof: If $\mathfrak{m} \subset \cup_j \mathfrak{p}_j$, then by Atiyah-Macdonald 1.11, we would have $\mathfrak{m} \subset \mathfrak{p}_j$ for some j. This would imply $\mathfrak{m} = \mathfrak{p}_j$, and so $\mathrm{ht}(\mathfrak{m}) = i-1 < d$, a contradiction.

So we may choose an element $x_i \in \mathfrak{m}$, $x_i \notin \cup_j \mathfrak{p}_j$. We claim that $x_1, \ldots, x_i$ satisfies (20.1.1).

Suppose that we have a prime $\mathfrak{q} \supset (x_1, \ldots, x_i)$. We need to show that $\mathrm{ht}(\mathfrak{q}) \geq i$. Clearly $\mathfrak{q} \supset \mathfrak{p}$, where the latter is some minimal prime containing $(x_1, \ldots, x_i)$.
Case 1: $\mathfrak{p} = \mathfrak{p}_j$, for some j. Then as $\mathfrak{q} \neq \mathfrak{p}_j$ (by choice of x_i), we have $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p}) + 1 = i$.
Case 2: $\mathfrak{p} \neq \mathfrak{p}_j$ for all j. Then $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{p}) \geq i$.

In summary, we have now proved the following fundamental theorem.

Theorem 20.1.2. *Let $(A,\mathfrak{m})$ be a Noetherian local ring. Then* $\dim A = d(A) = \delta(A)$. *In particular,* $\dim A < \infty$.

20.2. **Consequences of the dimension theorem for Noetherian local rings.** Recall that for any prime ideal in any ring A, we have $\mathrm{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$.

Corollary 20.2.1. *If A is Noetherian, and $\mathfrak{p}$ is a prime ideal, then* $\mathrm{ht}(\mathfrak{p}) < \infty$*, and therefore prime ideals in A satisfy the d.c.c. (descending chain condition: all descending chains are eventually stationary).*

Example: It is clear that the Noetherian hypothesis is necessary: consider $A = k[X_1, X_2, X_3, \dots]$ the polynomial ring in infinitely many variables. Then the chain of prime ideals

$$(X_1, X_2, X_3, \dots) \supsetneq (X_2, X_3, X_4, \dots) \supsetneq (X_3, X_4, X_5, \dots) \cdots$$

is not stationary.

Corollary 20.2.2. *If $(A, \mathfrak{m})$ is Noetherian local, and $k := A/\mathfrak{m}$, then* $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Proof. Indeed, NAK implies that $\mathfrak{m}$ is generated by at most $\dim_k \mathfrak{m}/\mathfrak{m}^2$ elements. □

Corollary 20.2.3. *If A is Noetherian, then any minimal prime $\mathfrak{p} \supset (x_1, \dots, x_r)$ has* $\mathrm{ht}(\mathfrak{p}) \leq r$.

Proof. The ideal $(x_1, \dots, x_r)$ becomes $\mathfrak{p}A_{\mathfrak{p}}$-primary in $A_{\mathfrak{p}}$. So the result follows from the inequality $\dim A_{\mathfrak{p}} \leq r$. □

Corollary 20.2.4 (Krull's Hauptidealsatz)**.** *Let A be a Noetherian ring, and $x \in A$ neither a unit nor a zero-divisor. Then every minimal prime $\mathfrak{p} \supset (x)$ has* $\mathrm{ht}(\mathfrak{p}) = 1$.

Proof. By the preceding corollary, $\mathrm{ht}(\mathfrak{p}) \leq 1$. If $\mathrm{ht}(\mathfrak{p}) = 0$, then $\mathfrak{p}$ belongs to 0, and thus every element in $\mathfrak{p}$ is a zero-divisor (Lemma 12.1.1, (b)), a contradiction. □

Corollary 20.2.5. *If $(A, \mathfrak{m})$ is Noetherian local, and $x \in \mathfrak{m}$ is not a zero-divisor, then* $\dim A/(x) = \dim A - 1$.

Proof. We have already proved, just a few paragraphs ago, that $d(A/(x)) \leq d(A) - 1$, and so $\leq$ holds. To prove the opposite inequality, write $d = \dim A/(x)$, and suppose $\overline{x}_1, \dots, \overline{x}_d$ generate an $\mathfrak{m}/(x)$-primary ideal. It follows that $I := (x, x_1, \dots, x_d)$ is $\mathfrak{m}$-primary: if the only prime ideal containing $I/(x)$ is $\mathfrak{m}/(x)$, then the only prime ideal containing I is $\mathfrak{m}$. Hence $d + 1 \geq \dim A$, as desired. □

Corollary 20.2.6. *Let $(\widehat{A}, \widehat{\mathfrak{m}})$ denote the $\mathfrak{m}$-adic completion of $(A, \mathfrak{m})$. Then* $\dim A = \dim \widehat{A}$.

Proof. Since $A/\mathfrak{m}^n \cong \widehat{A}/\widehat{\mathfrak{m}}^n$ for all $n \geq 0$, we have $\delta(A) = \delta(\widehat{A})$. □

Example: We have $\dim k[[X_1, \dots, X_n]] = n$. In the corollary above, take $A = k[X_1, \dots, X_n]_{\mathfrak{m}}$, where $\mathfrak{m} = (X_1, \dots, X_n)$, and observe that $k[[X_1, \dots, X_n]]$ is the $\mathfrak{m}$-adic completion of A.

21. Lecture 21

When a Noetherian domain is a UFD. Definition of regular local rings.
****

21.1. **Applications, in particular of Krull's Hauptidealsatz.** Recall: for A a domain, we define

- $a \neq 0$ is **irreducible** if $a \notin A^\times$ and a is not the product of two non-units.
- A is a **UFD** if each $a \neq 0$ is the pruduct of a unit and finitely many irreducible elements, uniquely up to units and reordering.

Lemma 21.1.1. *A Noetherian domain A in which every irreducible element generates a prime ideal is a UFD.*

Proof. First we need to show the existence of factorizations.

Consider the family of (principal) ideals

$$\mathcal{S} := \{0 \neq (a) \mid a \text{ is not the product of finitely many irred. elements}\}.$$

If $\mathcal{S} \neq \emptyset$, then $\mathcal{S}$ has a maximal element (a). The element a is neither a unit nor irreducible. So $a = a_1 a_2$, where a_i is a non-unit. We have $(a) \subsetneq (a_i)$, for $i = 1, 2$, and by maximality both a_i are products of finitely many irreducible elements. Hence so is a, a contradiction.

Therefore, given a, we may write $a = ua_1 \cdots a_r$, where $u \in A^\times$ and each a_i is irreducible. To prove uniqueness, assume

$$ua_1 \cdots a_r = vb_1 \cdots b_s$$

where $v \in A^\times$ and each b_j is irreducible. Since $vb_1 \cdots b_s \in (a_1)$ (a prime ideal by hypothesis), WLOG $b_1 \in (a_1)$. Thus

$$(b_1) \subset (a_1);$$

this is an inclusion of prime ideals by hypothesis, and such primes are ht 1, by Corollary 20.2.4. Thus $(b_1) = (a_1)$.[7] Thus WLOG $b_1 = a_1$ (absorbing a unit into v, say), and then we may cancel these from both sides. Continuing, the uniqueness statement follows. □

Theorem 21.1.2. *A Noetherian domain A is a UFD iff every prime of ht 1 is principal.*

Proof. ($\Leftarrow$): Suppose $\pi \in A$ is irreducible. By the preceding lemma, it's ETS (π) is prime. Let $\mathfrak{p} \supset (\pi)$ be a minimal prime ideal. Corollary 20.2.4 implies $\mathrm{ht}(\mathfrak{p}) = 1$, and so $\mathfrak{p}$ is principal by hypothesis, say $\mathfrak{p} = (a)$. Then (as noted in the footnote above) $(\pi) = (a)$ and so (π) is indeed prime.
($\Rightarrow$): Suppose $\mathrm{ht}(\mathfrak{p}) = 1$. Choose $x \neq 0$, $x \in \mathfrak{p}$. WLOG (factor x), we can assume x is irreducible. Note that because A is a UFD, (x) is then a prime ideal (check this!).

Then $(0) \subsetneq (x) \subset \mathfrak{p}$, and (x) is prime, so $\mathrm{ht}(\mathfrak{p}) = 1 \implies (x) = \mathfrak{p}$, and $\mathfrak{p}$ is principal, as desired. □

The following fact is important in number theory.

Corollary 21.1.3. *Let A be a Dedekind domain (i.e. a Noetherian normal domain of dimension 1). Then TFAE:*

(1) *A is a UFD.*
(2) *Every non-zero prime ideal in A is principal.*

[7] We can also argue as follows: note that if b is irreducible, then the ideal (b) is a maximal element in the collection of all *proper principal* ideals; this shows $(b_1) = (a_1)$, without invoking Krull's Hauptidealsatz (pointed out in class by Moshe Adrian).

(3) *A is a PID.*

Proof. (1) $\Leftrightarrow$ (2): Note that a prime ideal is non-zero iff it has ht 1.
(2) $\Leftrightarrow$ (3): Every proper non-zero ideal $\mathfrak{a}$ is product of non-zero prime ideals $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$. Hence every such $\mathfrak{a}$ is principal if and only if every non-zero prime ideal is principal. □

Aside: The geometric meaning of the Theorem (see Hartshorne II, Prop. 6.2): Let A be a Noetherian domain. and $X = \mathrm{Spec}(A)$. Then A is a UFD iff A is normal and $\mathrm{Div}(X)/(\text{principal divisors}) = \{0\}$.

21.2. **Definition of regular local ring.** Throughout this subsection, let $(A, \mathfrak{m})$ denote a Noetherian local ring, with residue field $k = A/\mathfrak{m}$. Let $d = \dim A$.

Theorem 21.2.1. *TFAE:*

(i) $G_{\mathfrak{m}}(A) \cong k[t_1, \ldots, t_d]$ *as graded k-algebras (the t_i's are indeterminates).*
(ii) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = d$.
(iii) $\mathfrak{m}$ *can be generated by d elements.*

We call a Noetherian local ring A a **regular local ring** if the equivalent conditions (i)-(iii) hold.

For the proof, note that $(i) \Rightarrow (ii)$ is clear, and $(ii) \Rightarrow (iii)$ follows by NAK.

Before giving the proof of $(iii) \Rightarrow (i)$, we need some preliminaries. First, we call any set of d elements $x_1, \ldots, x_d$ which generate an $\mathfrak{m}$-primary ideal a **system of parameters**. Choose such a system and set $I = (x_1, \ldots, x_d)$.

Lemma 21.2.2. *Let $\overline{x}_1, \ldots, \overline{x}_d \in I/I^2$. Let $f(t_1, \ldots, t_d) \in A[t_1, \ldots, t_d]$ be homogeneous of degree s. If $f(x_1, \ldots, x_d) \in I^{s+1}$, then $f \in \mathfrak{m}[t_1, \ldots, t_d]$.*

Proof. Let $\overline{f}(t_1, \ldots, t_d) \in A/I[t_1, \ldots, t_d]$ denote the image of f modulo I. There is a surjective graded A/I-algebra homomorphism

$$\alpha : A/I[t_1, \ldots, t_d] \twoheadrightarrow G_I(A)$$

given by $t_i \mapsto \overline{x}_i$, for $i = 1, \ldots, d$. By assumption $\overline{f} \in \ker(\alpha)$.

Assume that not all coefficients of f belong to $\mathfrak{m}$; then some coefficient of f is a unit, and so (check this!), $\overline{f}$ is not a zero-divisor in $A/I[t_1, \ldots, t_d]$. Then we have

$$\begin{aligned} d = d(G_I(A)) &\leq^* d(A/I[t_1, \ldots, t_d]/(\overline{f})) \\ &= d(A/I[t_1, \ldots, t_d]) - 1 \\ &= d - 1, \end{aligned}$$

which is a contradiction. We are done, modulo the inequality $\leq^*$ above. This follows from the following general lemma. □

Lemma 21.2.3. *Let $M = \oplus_n M_n \twoheadrightarrow N = \oplus_n N_n$ be a surjective homomorphism of graded modules over the graded ring $A/I[t_1, \ldots, t_d]$. Then $\ell_{A/I}(N_n) \leq \ell_{A/I}(M_n)$, and thus $d(N) \leq d(M)$.*

Proof. Note that $d(N) - 1 = \deg_n \ell(N_n)$, and similarly for M replacing N. □

Proof of Theorem 21.2.1, $(iii) \Rightarrow (i)$: Suppose $\mathfrak{m} = (x_1, \ldots, x_d)$. Define the graded $A/\mathfrak{m}$-algebra surjective homomorphism

$$A/\mathfrak{m}[t_1, \ldots, t_d] \twoheadrightarrow G_{\mathfrak{m}}(A)$$

by $t_i \mapsto \overline{x}_i \in \mathfrak{m}/\mathfrak{m}^2$. By Lemma 21.2.2, this is injective, hence is an isomorphism. □

Corollary 21.2.4. *Suppose $(\widehat{A}, \widehat{\mathfrak{m}})$ is the $\mathfrak{m}$-adic completion of the Noetherian local ring $(A, \mathfrak{m})$. Then A is regular iff $\widehat{A}$ is regular.*

Proof. Indeed, we have $G_{\mathfrak{m}}(A) = G_{\widehat{\mathfrak{m}}}(\widehat{A})$, and so the latter is a polynomial ring over k in $d = \dim(A) = \dim(\widehat{A})$ variables. □

As a corollary of Lemma 21.2.2 above, we have the following result we will use later.

Corollary 21.2.5. *Suppose A contains a field k mapping isomorphically onto $A/\mathfrak{m}$. Then any system of parameters $x_1, \ldots, x_d$ is algebraically independent over k.*

Proof. Let I be the ideal generated by the elements $x_1, \ldots, x_d$. Suppose $(x_1, \ldots, x_d)$ is a zero of $0 \neq f(t_1, \ldots, t_d) \in k[t_1, \ldots, t_d]$. Write $f = f_s + (\deg > s \text{ terms})$, where $f_s \neq 0$ is homogeneous of degree s. Then $f_s(x_1, \ldots, x_d) \in I^{s+1}$, and so by Lemma 21.2.2, all coefficients of f_s belong to $k \cap \mathfrak{m} = 0$, a contradiction. □

21.3. **Regular local rings are domains, and a consequence.**

Proposition 21.3.1. *If A is a regular local ring, then A is a domain.*

This follows from the next lemma.

Lemma 21.3.2. *Let A be any ring and I is an ideal such that $\cap_{n\geq 1} I^n = 0$. Assume that $G_I(A)$ is a domain. Then A is a domain.*

Proof. If $x, y \neq 0$, then there exist non-negative integers n, m with $x \in I^n - I^{n+1}$ and $y \in I^m - I^{m+1}$. So $0 \neq \overline{x} \in I^n/I^{n+1}$ and $0 \neq \overline{y} \in I^m/I^{m+1}$. Since $G_I(A)$ is a domain, it follows that $0 \neq \overline{xy} \in I^{n+m}/I^{n+m+1}$. Thus $xy \neq 0$. □

Here is a nice consequence:

Corollary 21.3.3. *The dimension 1 regular local Noetherian rings are precisely the dimension 1 local Noetherian domains such that $\mathfrak{m}$ is principal, ie., the DVR's.*

By a **curve** we mean a 1-dimensional variety over a field k. We usually assume $k = \overline{k}$, though this is not always necessary. We say a curve X is **regular** if every local ring $\mathcal{O}_x$ is regular, for every closed point x. The above corollary means that an *irreducible* curve X is regular iff it is normal (meaning each $\mathcal{O}_x$ is normal).

22. Lecture 22

More dimension theory. Comparison of regular local rings with non-singular points on alg. var.

****

22.1. **More dimension theory.** We can now give the proof of a fact we mentioned earlier (Proposition 7.6.1).

"if": Since f is irreducible and $k[X_1, \ldots, X_n]$ is a UFD, the ideal (f) is prime, call it P. Because any maximal chain of prime ideals in $k[X_1, \ldots, X_n]$ has length n, we know that

$$\mathrm{ht}(P) + \dim(A/P) = n.$$

By Krull's Hauptidealsatz, $\mathrm{ht}(P) = 1$, and so $\dim(Y) = \dim(A/P) = n - 1$.

"only if": Since Y is closed and irreducible, $Y = V(P)$ for some prime ideal P. Since $\dim(Y) = n-1$, the above reasoning shows that $\mathrm{ht}(P) = 1$. Since $k[X_1, \dots, X_n]$ is a UFD, P is principal, say $P = (f)$. Since P is prime, f must be irreducible. □

Our next goal is to prove a related result, where $k[X_1, \dots, X_n]$ is replaced with an arbitrary f.g. k-algebra which is a domain.

Proposition 22.1.1. *Suppose $k = \overline{k}$. Let A be a f.g. k-algebra, which is a domain. Suppose $f \in A$, $f \notin A^\times$, $f \neq 0$. Let $d = \dim(A)$. Then $V(f) = \mathrm{Spec}(A/(f))$ is pure of dimension $d-1$.*

To say that $V(f)$ is **pure of dimension** $d-1$ means, by definition, that all the irreducible components of $\mathrm{Spec}(A/(f))$ have dimension $d-1$.

Proof. Let $Z_1, \dots, Z_l$ be the irreducible components of $V(f) = \mathrm{Spec}(A/(f))$. Then $Z_i = V(P_i)$, where P_i ranges over the finite set of minimal primes $P_i \supset (f)$. By Krull's Hauptidealsatz, $\mathrm{ht}(P_i) = 1$ for each i, and from the equality

$$\mathrm{ht}(P_i) + \dim(A/P_i) = \dim(A) = d$$

we get $\dim(Z_i) = \dim(A/P_i) = d-1$, for each i. □

Here is another useful result.

Proposition 22.1.2. *Suppose $A = k[X_1, \dots, X_n]/(f_1, \dots, f_t)$, and $(f_1, \dots, f_t) \neq (1)$. Then $\dim(A) \geq n - t$.*

Proof. An irreducible component of $\mathrm{Spec}(A)$ is of the form $V(P) \subset \mathrm{Spec}(k[X_1, \dots, X_n])$ where $P \supset (f_1, \dots, f_t)$ is minimal. We have the equality

$$\mathrm{ht}(P) + \dim(V(P)) = n.$$

On the other hand, we know that $\mathrm{ht}(P) \leq t$. Putting these together, we find

$$\dim(V(P)) \geq n - t.$$

Since $\dim(A) = \sup_P \dim(V(P))$, the desired inequality follows. □

We say a closed irreducible subset $Y \subset \mathbb{A}^n_k$ as above is a **local complete intersection** if there exist $f_1, \dots, f_t \in k[X_1, \dots, X_n]$ such that $I(Y) = (f_1, \dots, f_t)$ and

$$\dim Y = n - t.$$

22.2. **Regularity vs non-singularity.** The following comparison between regularity of local rings and non-singularity of points on varieties is taken from Hartshorne, I §5.

Fix $k = \overline{k}$, and a closed subvariety $Y \subset \mathbb{A}^n_k$ (i.e. a Zariski-closed subset of $\mathrm{Spec}(k[X_1, \dots, X_n])$, which is **reduced**: we can write $Y = V(I(Y))$ where $I(Y) \subset k[X_1, \dots, X_n]$ is a radical ideal; then $Y \cong \mathrm{Spec}(k[X_1, \dots, X_n]/I(Y))$ and the ring of regular functions on Y, namely $\mathcal{O}_Y := k[X_1, \dots, X_n]/I(Y)$ has no non-zero nilpotents). Suppose in addition that Y is irreducible: this means $I(Y)$ is a prime ideal.

Write $I(Y) = (f_1, \dots, f_t)$.

Suppose the closed point $P = (a_1, \dots, a_n)$ belongs to Y, i.e. $(X_1 - a_1, \dots, X_n - a_n) \supset I(Y)$. Then we say Y **is non-singular at** P if

$$\mathrm{rank}\ J(P) = n - \dim(Y), \tag{22.2.1}$$

where J denotes the **Jacobian matrix**

$$J = \Big(\frac{\partial f_i}{\partial X_j}\Big)_{ij}$$

a $t \times n$ matrix with entries which belong to $k[X_1, \ldots, X_n]$, so may be evaluated at the point P, yielding $J(P)$.

Remark 22.2.1.
- *In order for the definition to make sense, we must have* $n - \dim\, Y \leq \min\{t, n\}$. *But* $Y \neq \emptyset \implies (f_1, \ldots, f_t) \neq (1)$, *and then* $n - \dim\, Y \leq t$ *follows from Proposition 22.1.2.*
- *The definition appears to depend on the choice of the generators* $f_1, \ldots, f_t$ *for* $I(Y)$. *We shall see below that in fact it does not.*
- *We shall see below that we always have the inequality* rank $J(P) \leq n - \dim(Y)$, *so saying the* P *is a non-singular point of* Y *is saying that the rank of* $J(P)$ *is as large as possible.*

Let us denote the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$ corresponding to P by $\mathfrak{a}_P \in \mathrm{Spec}_{\mathfrak{m}}\ k[X_1, \ldots, X_n]$. Let $\mathfrak{m} \in \mathrm{Spec}_{\mathfrak{m}}(\mathcal{O}_Y)$ denote the image of $\mathfrak{a}_P$ under the projection $k[X_1, \ldots, X_n] \twoheadrightarrow \mathcal{O}_Y$. We use the same symbol $\mathfrak{m}$ to denote the maximal ideal in the local ring $A := \mathcal{O}_{Y,\mathfrak{m}}$.

Theorem 22.2.2. *Y is non-singular at P iff A is regular.*

Proof. For brevity write $k[X] = k[X_1, \ldots, X_n]$.
Claim 1: There is a k-linear isomorphism $\theta' : \mathfrak{a}_P/\mathfrak{a}_P^2 \xrightarrow{\sim} k^n$.
Proof: Define $\theta : k[X] \to k^n$ by

$$\theta(f) = \Big[\frac{\partial f}{\partial X_1}(P), \ldots, \frac{\partial f}{\partial X_n}(P)\Big].$$

It is clear that $\theta(\mathfrak{a}_P^2) = 0$. Also, the image of the set $\{X_i - a_i\}_i$ gives a k-basis for $\mathfrak{a}_P/\mathfrak{a}_P^2$, which is taken by θ to the standard basis of k^n. Hence θ induces the isomorphism θ'.

Claim 2: rank $J(P) = \dim_k\, \theta(I(Y)) = \dim_k\, \dfrac{I(Y) + \mathfrak{a}_P^2}{\mathfrak{a}_P^2}$.

Proof: Any $h \in I(Y)$ can be written in the form $h = g_1 f_1 + \cdots + g_t f_t$, for some $g_i \in k[X]$. We have $\theta(h) = g_1(P)\theta(f_1) + \cdots g_t(P)\theta(f_t)$, which shows that the rows of $J(P)$ span $\theta(I(Y))$. The first equality follows.

For the second equality, note that $\theta(I(Y)) = \frac{I(Y)}{I(Y) \cap \mathfrak{a}_P^2} \cong \frac{I(Y) + \mathfrak{a}_P^2}{\mathfrak{a}_P^2}$.

Claim 3: $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{a}_P/(I(Y) + \mathfrak{a}_P^2)$, as k-vector spaces.
Proof: We have

$$\begin{aligned} \mathfrak{m} &= \mathfrak{a}_{P\mathfrak{a}_P}/I(Y)_{\mathfrak{a}_P} \\ \mathfrak{m}^2 &= (\mathfrak{a}_P^2 + I(Y))_{\mathfrak{a}_P}/I(Y)_{\mathfrak{a}_P}, \text{ and thus} \\ \mathfrak{m}/\mathfrak{m}^2 &= (\mathfrak{a}_P/(\mathfrak{a}_P^2 + I(Y)))_{\mathfrak{a}_P}, \end{aligned}$$

which is just $\mathfrak{a}_P/(\mathfrak{a}_P^2 + I(Y))$.

Putting Claims 1-3 together, we get

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 + \text{rank } J(P) = n. \tag{22.2.2}$$

This equation implies the theorem. Indeed, recall that since $\mathcal{O}_Y$ is a f.g. k-algebra and a domain, we have dim Y = dim A. Write r for this dimension. Then

the ring A is regular iff $\dim_k \mathfrak{m}/\mathfrak{m}^2 = r$ which by (22.2.2) holds iff rank $J(P) = n - r$. $\square$

We also see that since we always have the inequality $\dim Y \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$, equation (22.2.2) implies that we always have the inequality

$$\text{rank } J(P) \leq n - \dim Y. \tag{22.2.3}$$

In particular, the point P is **singular** (ie. not non-singular) if and only

$$\text{rank } J(P) < n - \dim Y.$$

Examples:

- If $Y \subset \mathbb{A}^n_k$ is cut out by a single non-zero non-unit element $f \in k[X]$, then $P \in Y$ is non-singular iff $J(P) \in k^n$ is not the zero vector.
- For the curves cut out by $X^2 - Y^3$ and $X^2 - Y^2 + X^3$ in the plane $\mathbb{A}^2$, the only singularity in each case is $P = (0, 0)$, as is easily checked.

Exercise 22.2.3. *Let Y be an irreducible (affine) variety, that is, in the affine case $Y = \text{Spec}(A)$ where A is a f.g. domain over an algebraically field k. Show that the set* Sing(Y) *of singular points is a proper Zariski-closed subset of Y. [See Hartshorne,* Algebraic Geometry*, II, §8, Cor. 8.16.]*

Exercise 22.2.4. *Let Y be an irreducible hypersurface in $\mathbb{A}^n_k$, i.e. $Y = V(f)$, where $f \in k[X_1, \ldots, X_n]$ is an irreducible element. Show that* $\text{Sing}(Y) = V(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n})$. *Show that the singularities are* isolated*, meaning that* $\dim \text{Sing}(Y) = 0$*, if and only the k-vector space $k[X_1, \ldots, X_n]/(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n})$ is finite-dimensional.*

As a final remark, let $(x_1, \ldots, x_d) = \mathfrak{m}$ denote a system of parameters in a d-dimensional regular local ring $(A, \mathfrak{m})$, where A is also a $k := A/\mathfrak{m}$-algebra (for example, A could be a localization at a maximal ideal of a f.g. k-algebra). Then we can define a k-algebra homomorphism

$$\phi : k[t_1, \ldots, t_d] \to A$$

by sending $t_i \mapsto x_i$, for $i = 1, \ldots, d$. This induces an isomorphism

$$G(\phi) : k[t_1, \ldots, t_d] \xrightarrow{\sim} G_{\mathfrak{m}}(A).$$

Hence by Lemma 18.2.2, the induced map $\widehat{\phi}$ on completions is also an isomorphism:

$$\widehat{\phi} : k[[t_1, \ldots, t_d]] \xrightarrow{\sim} \widehat{A}.$$

This proves the following result.

Proposition 22.2.5. *If $P \in Y$ is any non-singular point on a d-dimensional irreducible variety Y, there is an isomorphism*

$$k[[t_1, \ldots, t_d]] \cong \widehat{\mathcal{O}_{Y,P}}.$$

22.3. **Some deeper connections of regularity with geometry.** If $X = \text{Spec}(A)$, where A is a Noetherian domain, we say X is **regular** if $A_{\mathfrak{m}}$ is a regular local ring for every maximal ideal $\mathfrak{m} \in \text{Spec}_{\mathfrak{m}}(A)$. Similarly, we say X is **normal** if $A_{\mathfrak{m}}$ is normal for all $\mathfrak{m}$. (We already know that this is equivalent to saying A is normal, even without the assumption that A be Noetherian.) Similar terminology applies to reduced and irreducible schemes.

Fact 1: Assume $(A, \mathfrak{m})$ is a regular local ring (hence a domain). Then A is normal. Thus, a regular scheme is normal.

In fact, a much stronger result is true: any regular local ring is a UFD (the Auslander-Buchsbaum theorem). The proof of this is beyond the scope of this course. We will prove Fact 1 in the next lecture.

Fact 2: Any normal scheme is regular in codimension 1.

What does "regular in codim 1 mean"? Let us discuss this in the affine case, i.e. where A is a Noetherian domain. Then $X = \mathrm{Spec}(A)$ is **regular in codimension 1** if for any height 1 prime ideal $P \subset A$, the ring A_P is *regular*. Now the proof of Fact 2 is almost trivial: the ring A_P is a Noetherian local domain of dimension 1, and if A is normal, A_P is also normal; thus, A_P is a DVR, hence is regular.

Fact 2 can be used to prove the following proposition.

Proposition 22.3.1 (Consequence of Fact 2)**.** *If X is a normal variety, and* $\mathrm{Sing}(X) \subset X$ *is the (Zariski-closed) set of singular points, then* $\mathrm{codim}(\mathrm{Sing}(X)) \geq 2$*. In particular, any normal curve is non-singular, and any normal surface has only isolated singularities.*

A key ingredient of the proof is a theorem of Serre which states that if A is regular, then so is $A_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$ (see [Serre], IV.D.Prop.23). We will not prove this, but it is quite important.

Many interesting singular varieties are normal: for example Schubert varieties are usually singular, but they are at least always normal. We shall give some concrete examples next lecture.

23. Lecture 23

Proof that A regular implies A is normal (using almost integral extensions). Example of $k[X, Z]/(Z^2 - f)$. Definition of module of relative differentials: construction of the universal derivation.

****

23.1. **Proof that "regular" implies "normal".** We will now prove Fact 1 from the previous lecture. We will follow the treatment in [Mat1],17.D, p.119.

Proposition 23.1.1. *If A is a regular local ring, then A is normal.*

To prove this, we need some preliminaries. Temporarily, we let A denote any domain, with $K = \mathrm{Frac}(A)$.

We say $u \in K^\times$ is **almost integral** if $\exists\, 0 \neq a \in A$ such that $au^n \in A$, $\forall n > 0$. We abbreviate "almost integral" by **a.i.** Note that u, v a.i. implies that uv and $u \pm v$ are also a.i.

Lemma 23.1.2. (i) *If u is integral, it is a.i.*

(ii) *The converse holds if A is Noetherian.*

Proof. (i): Write $u = a/b$, for $a, b \in A - 0$. Consider a relation

$$\Big(\frac{a}{b}\Big)^n + \alpha_{n-1}\Big(\frac{a}{b}\Big)^{n-1} + \cdots + \alpha_0 = 0,$$

where $\alpha_i \in A$ for all i. Then it is easy to see that $b^{n-1}\Big(\frac{a}{b}\Big)^k \in A$, for all $k > 0$. Hence u is a.i.

(ii): If u is a.i. with $au^n \in A$ for all $n > 0$, we have an inclusion $A[u] \subset a^{-1}A$. Then since A is Noetherian, the $A[u]$ is a finite A-module. It follows that u is integral over A. □

Now to prove the proposition above, it is enough to establish the implication "$G_{\mathfrak{m}}(A)$ normal domain $\implies$ A normal domain". We will prove something more general.

Proposition 23.1.3. *Suppose A is a Noetherian ring, with $I \subset A$ an ideal belonging to the Jacobson radical. Then*

$$G_I(A) \text{ is a normal domain } \implies A \text{ is a normal domain.}$$

Proof. As a consequence of Krull's theorem, we know that $\cap_{n=0}^{\infty} I^n = 0$. So for $0 \neq a \in A$ there is a unique non-negative integer n with $a \in I^n - I^{n+1}$. Denote $\mathrm{ord}(a) = n$, and let a^* be the image of a in I^n/I^{n+1}. By convention, set $0^* = 0 \in G_I(A)$.

We already know that A is a domain; let $K = \mathrm{Frac}(A)$. Suppose $a/b \in K^\times$ is integral. We want to show that $a \in bA$. Since A/bA is Hausdorff in the I-adic topology, we have

$$bA = \cap_{n=0}^{\infty}(bA + I^n).$$

Hence, it's ETS the implication

$$a \in bA + I^{n-1} \implies a \in bA + I^n. \tag{23.1.1}$$

Write $a = br + a'$, where $r \in A$ and $a' \in I^{n-1}$. This gives $a'/b = a/b - r$, which is integral over A. Hence by replacing a with a' we may assume WLOG that $a \in I^{n-1}$.

Now a/b a.i. means that $\exists 0 \neq c \in A$ such that $ca^m \in b^m A$, for all $m > 0$. Since $G_I(A)$ is a domain, the map $x \mapsto x^*$ is multiplicative, so we have $c^*(a^*)^m \in (b^*)^m G_I(A)$. Hence $a^*/b^* \in G_I(A)$ is a.i. Since $G_I(A)$ is Noetherian, this shows that a^*/b^* is integral. But then since $G_I(A)$ is normal, we have $a^* \in b^* G_I(A)$.

Write $a^* = b^* d^*$, for some element $d \in A$ (check: we can do this). Then we have $a^* = (bd)^*$, and so

$$n - 1 \leq \mathrm{ord}(a) < \mathrm{ord}(a - bd),$$

which implies that $a \in bd + I^n$, as desired. This completes the proof. □

23.2. **The varieties cut out by $Z^2 - f$.** Again let $k[X] = k[X_1, \ldots, X_n]$. Suppose $f \in k[X]$ is not a square, so that $Z^2 - f \in k[X, Z]$ is irreducible. Some time ago we asked: when is the domain $A := k[X, Z]/(Z^2 - f)$ normal? Here is the answer:

Proposition 23.2.1. *Assume* char $k \neq 2$. *Then A is normal iff f is square-free.*

Proof. ($\Rightarrow$) : Suppose f is not-square free. We will produce an element in the fraction field of A but not in A, which is a.i. (hence integral over A). This will show that A is not normal.

Write $f(X) = h(X)g(X)^2$. Then we claim that $Z/g(X)$ is a.i. Indeed, note that for every $n \geq 0$ we have the following two equalities

$$g(X)\Big(\frac{Z}{g(X)}\Big)^{2n} = g(X)h(X)^n$$
$$g(X)\Big(\frac{Z}{g(X)}\Big)^{2n+1} = Zh(X)^n.$$

($\Leftarrow$): For this direction, we prove something more general.

Lemma 23.2.2. *Let R be a UFD in which 2 is a unit. Suppose $f \in R$ is square-free. Then $R[Z]/(Z^2 - f) = R[\sqrt{F}]$ is normal.*

Proof. Write $\alpha = \overline{Z} = \sqrt{f}$. Then $K := \text{Frac } R \subset \text{Frac } R[\alpha]$, and α is an element of the latter.

If $\alpha \in K$, then $\alpha \in R$ (since R is normal), and this contradicts the assumption that f is not a square. So $\alpha \notin K$, and so $K(\alpha) = K[\alpha] = K + K\alpha$.

Suppose $\lambda = x + y\alpha \in K(\alpha)$ $(x, y \in K)$ is integral over $A[\alpha]$. We will show that $x, y \in R$, showing that $R[\alpha]$ is normal.

First, WLOG $y \neq 0$. Indeed, if $y = 0$, then x is integral over R, hence $x \in R$. Now the minimal polynomial for λ over K takes the form

$$\min_K(\lambda) = X^2 - 2xX + (x^2 - y^2 f).$$

Now λ is integral over $R[\lambda]$ (thus over R) $\Leftrightarrow 2x, x^2 - y^2 f \in R$, which holds $\Leftrightarrow x, -y^2 f \in R$. So the latter holds.

We claim that $y \in R$. If π is an irreducible element of R and π divides the denominator of y, then $-y^2 f \in R$ implies that π^2 divides f, a contradiction of f being square-free. Thus $y \in R$ and the lemma is proved. □

The lemma clearly implies the direction ($\Leftarrow$) of the proposition. □

The following exercise gives some very concrete examples of varieties which are normal and singular.

Exercise 23.2.3. *Suppose that $f(X_1, \ldots, X_n) = (X_1 - a_1)(X_2 - a_2)$, where $a_1 \neq a_2$. Let $Y = \text{Spec}(k[X, Z]/(Z^2 - f))$. By the above proposition, Y is a normal irreducible variety. Show that Y has a singularity at any point of the form $(a_1, a_2, x_3, \ldots, x_n, 0)$. What is the dimension of the singular locus? What is its codimension in Y?*

23.3. **Derivations and the module of Kähler differentials.** We will develop the algebraic theory of differential 1-forms. We actually develop a "relative" version, i.e. we fix a ring k, and a k-algebra A (that is, a ring A with a ring homomorphism $k \to A$). We will define an A-module $\Omega_{A/k} = \Omega^1_{A/k}$, which is uniquely determined in a certain sense.

To do so, we first fix an A-module M and define the set $\text{Der}_k(A, M)$ of k-derivations $A \to M$. What is a k-derivation? It is a k-linear map $D : A \to M$ satisfying the **Leibniz rule:**

$$D(ab) = aDb + bDa.$$

The set $\text{Der}_k(A, M)$ is naturally an A-module: $(aD)(b) := a(Db)$. Also, an A-linear map $\phi : M \to M'$ gives rise to $\text{Der}_k(A, M) \to \text{Der}_k(A, M')$ by $D \mapsto \phi \circ D$.

Theorem 23.3.1. *The covariant functor $M \mapsto \text{Der}_k(A, M)$ is represented by a unique pair (M_0, d):*

- *$d : A \to M_0$ is a k-derivation;*
- *For every k-derivation $D : A \to M$, there exists a unique A-homomorphism $\phi : M_0 \to M$ such that $D = \phi \circ d$.*

The pair (M_0, d) is unique up to a unique isomorphism. We denote M_0 by $\Omega_{A/k}$ and call it the **module of relative differentials**. The theorem gives a (functorial in M) isomorphism

$$\text{Der}_k(A, M) = \text{Hom}_A(\Omega_{A/k}, M). \tag{23.3.1}$$

Construction of (M_0, d): Consider the A-algebra homomorphism

$$\mu : A \otimes_k A \to A$$

defined by $x \otimes y \mapsto xy$. Let $I := \ker(\mu)$. Let $\Omega_{A/k} := I/I^2$. The exact sequence

$$0 \longrightarrow I/I^2 \longrightarrow A \otimes_k A/I^2 \xrightarrow{\mu'} A \longrightarrow 0$$

splits in A-Mod in two ways: $\lambda_1(a) := 1 \otimes a$, and $\lambda_2(a) := a \otimes 1$ both determine sections of μ'. Therefore the difference $\lambda_1 - \lambda_2$ has image in I/I^2, and since λ_i is a k-algebra map, the map

$$d := \lambda_1 - \lambda_2 : A \to I/I^2$$

is a k-derivation. Indeed, I/I^2 has A-module structure given by multiplication by either $1 \otimes a$ or $a \otimes 1$, so that $(\lambda_1 - \lambda_2)(ab) = \lambda_1(a)\lambda_1(b) - \lambda_2(a)\lambda_2(b)$ is the sum the following two expressions:

$$a(\lambda_1 - \lambda_2)(b) = \lambda_1(a)(\lambda_1(b) - \lambda_2(b))$$
$$b(\lambda_1 - \lambda_2)(a) = \lambda_2(b)(\lambda_1(a) - \lambda_2(a)).$$

The proof gives us a principle which we will use repeatedly:

Lemma 23.3.2. *Suppose $\lambda_1, \lambda_2 : A \to B$ are k-algebra homomorphisms, and assume $\lambda_1 - \lambda_2$ takes values in an A-submodule $N \subset B$ whose A-module structure is given by multiplication by $\lambda_1(a)$ and assume $\lambda_1(a) - \lambda_2(a)$ acts by zero on N. Then $\lambda_1 - \lambda_2 : A \to N$ is a k-derivation.*

We will complete the proof that $(\Omega_{A/k} := I/I^2, d)$ satisfies the universal property in the next lecture.

24. Lecture 24

24.1. **Universal property of** $(\Omega_{A/k}, d)$**.** We need a preliminary construction. If $M \in A$-Mod, we define a k-algebra $A * M$ by setting $A * M = A \oplus M$ and by defining multiplication by

$$(a, m)(a', m') := (aa', am' + a'm).$$

Clearly $A * M$ is a k-algebra with unit $(1, 0)$. The exact sequence

$$0 \to M \to A * M \to M \to 0$$

splits. The inclusion of M is given by $m \mapsto (0, m)$ and the projection onto A is $(a, m) \mapsto a$. The latter has the obvious section $a \mapsto (a, 0)$. Note also that $M^2 = 0$ in $A * M$.

Now given $D \in \mathrm{Der}_k(A, M)$ define $\phi : A \otimes_k A \to A * M$ by

$$\phi(x \otimes y) = (xy, xDy).$$

It is easy to check the following statements:

- ϕ is a k-algebra homomorphism;
- $\sum_i x_i \otimes y_i \in I \implies \phi(\sum_i x_i \otimes y_i) = (0, \sum_i x_i D y_i) \in M$. Therefore $\phi : I \to M \subset A * M$;
- Since $M^2 = 0$ in $A * M$, the map ϕ determines $\phi : I/I^2 \to M$.
- We have $\phi(da) = \phi(1 \otimes a - a \otimes 1) = (0, Da)$ (since $D1 = 0$), and thus $\phi \circ d = D$;

- ϕ is A-linear: $a(\sum_i x_i \otimes y_i) = \sum_i ax_i \otimes y_i \mapsto (0, \sum_i ax_i Dy_i) = a\phi(\sum_i x_i \otimes y_i)$.

We have now proved the *existence* of the factoring $\phi \circ d = D$.

It remains to prove that ϕ is the *unique* A-linear map with the property $\phi \circ d = D$. This will follow from the fact that $\Omega_{A/k}$ is generated over A by the set $\{da, a \in A\}$.

Why is this true? Observe that

$$a \otimes a' = (a \otimes 1)(1 \otimes a - a \otimes 1) + aa' \otimes 1.$$

So $\omega = \sum_i x_i \otimes y_i \in I \implies \omega \equiv \sum_i x_i dy_i$ in I/I^2. This completes the proof of the universal property of $(\Omega_{A/k}, d)$. □

24.2. **Examples.**

- Let A be a k-algebra, generated as an algebra by a subset $U \subset A$. Then $\Omega_{A/k}$ is generated over A by $da, a \in U$. To prove this, note that an element in A can be written in the form $a = f(a_1, \dots a_n)$ for some $a_i \in U$ and $f \in k[X_1, \dots, X_n]$. Our claim results from the following exercise.

  Exercise 24.2.1. *Show that Leibniz' rule implies*

$$da = \sum_i \frac{\partial f}{\partial X_i}(a_1, \dots, a_n)\ da_i. \tag{24.2.1}$$

- In particular, if $A = k[X_1, \dots, X_n]$, then $\Omega_{A/k} = AdX_1 + \cdots + AdX_n$. Moreover, we have $\Omega_{A/k} \cong A^n$, i.e., the dX_i's are linearly independent over A. To prove this, for each i let $D_i \in \mathrm{Der}_k(A, A)$ denote the k-derivation $D_i = \frac{\partial}{\partial X_i}$. This corresponds to the A-linear map $\phi_i : \Omega_{A/k} \to A$, such that $\phi_i \circ d = D_i$. Now if there is a relation, $a_1 dX_1 + \cdots + a_n dX_n = 0$, applying ϕ_i gives $a_i = 0$.

24.3. **0-smooth, 0-unramified, and 0-étale homomorphisms.** Let k be a ring, and let $k \to A$ be a k-algebra. We say A is **0-smooth** (over k) if for every k-algebra C and ideal $I \subset C$ such that $I^2 = 0$, if we are given a k-algebra map $u : A \to C/I$, then there is a lift of u to a k-algebra map $v : A \to C$. In other words, given a commutative square below, there is a map v making the triangles commute:

$$\begin{array}{ccc} A & \xrightarrow{u} & C/I \\ \uparrow & \overset{v}{\searrow} & \uparrow \\ k & \longrightarrow & C \end{array}$$

We say A is **0-unramified** if given u there is *at most one* such map v. We say A is **0-étale** if given u there is exactly one such v. Thus, 0-étale = 0-smooth + 0-unramified,

Lemma 24.3.1. *A/k is 0-unramified iff $\Omega_{A/k} = 0$.*

Proof. ($\Leftarrow$): Suppose v_1, v_2 are two lifts of u; give the ideal $I \subset C$ the structure of an A-module by multiplication by $v_1(a)$ (or $v_2(a)$: since $v_1(a) - v_2(a) \in I$ and $I^2 = 0$, the two structures coincide). Then by Lemma 23.3.2, $v_1 - v_2 : A \to I$ is a k-derivation. Since $\Omega_{A/k} = 0$, the only k-derivation $A \to I$ is zero, and so $v_1 = v_2$. This shows A/k is unramified.

($\Rightarrow$): Consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\lambda_i} & A \otimes_k A/I \\ \uparrow & \nearrow_{\overline{\lambda}_i} & \uparrow \\ k & \longrightarrow & A \otimes_k A/I^2. \end{array}$$

Since the maps $\lambda_i : A \to A \otimes_k A/I$ agree, by hypothesis so do the maps $\overline{\lambda}_i$. This means that the derivation $d := \overline{\lambda}_1 - \overline{\lambda}_2 : A \to \Omega_{A/k}$ is zero. Since $\Omega_{A/k}$ is generated over A by dA, we get $\Omega_{A/k} = 0$, as desired. □

Lemma 24.3.2. *Let $S \subset A$ be a multiplicative subset. Then $A_S := S^{-1}A$ is 0-étale over A.*

Proof. Consider the diagram

$$\begin{array}{ccc} A_S & \xrightarrow{u} & C/I \\ {\scriptstyle p}\uparrow & \nearrow_{\exists!} & \uparrow \\ A & \xrightarrow{q} & C. \end{array}$$

We want to produce the unique morphism $A_S \to C$ making the diagram commute. But *up* sends S into $(C/I)^\times$, so q sends S into $C^\times$ (note that $c \in C^\times$ iff its image $\overline{c} \in (C/I)^\times$, since $I^2 = 0$). Thus, q factorizes uniquely through A_S, as desired. □

24.4. **The First Fundamental Exact Sequence.** The next result is the *First Fundamental Exact sequence.*

Theorem 24.4.1. *Let $k \xrightarrow{f} A \xrightarrow{g} B$ be two ring homomorphisms.*

(1) *There is an exact sequence of B-modules*

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0, \tag{24.4.1}$$

where $\alpha(d_{A/k}a \otimes b) = bd_{B/k}g(a)$, and $\beta(d_{B/k}b) = d_{B/A}b$

(2) *If B is 0-smooth over A, then*

$$0 \longrightarrow \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0 \tag{24.4.2}$$

is split exact.

Proof. (1): By a standard argument (see Atiyah-Macdonald, 2.9), $N' \to N \to N''$ is exact in B-Mod iff for every $T \in B$-Mod, $\mathrm{Hom}_B(N'.T) \leftarrow \mathrm{Hom}_B(N, T) \leftarrow \mathrm{Hom}_B(N'', T)$ is exact. Therefore, it's ETS: for every $M \in B$-Mod, the following diagram is commutative with exact first row:

$$\begin{array}{ccccccc} \mathrm{Der}_k(A,M) & \xleftarrow{rest.} & \mathrm{Der}_k(B,M) & \xleftarrow{incl.} & \mathrm{Der}_A(B,M) & \longleftarrow & 0 \\ \| & & \| & & \| & & \\ \mathrm{Hom}_B(\Omega_{A/k} \otimes_A B, M) & \xleftarrow{\alpha^*} & \mathrm{Hom}_B(\Omega_{B/k}, M) & \xleftarrow{\beta^*} & \mathrm{Hom}_B(\Omega_{B/A}, M) & \longleftarrow & 0. \end{array}$$

(The exactness of the first row is easy; check the diagram commutes, where α, β are defined as in the statement of (1)!)

(2): Suppose B is 0-smooth over A. Fix $T \in B$-Mod, and $D \in \mathrm{Der}_k(A,T)$. Consider the diagram

$$\begin{array}{ccc} B & \xrightarrow{id} & B \\ {\scriptstyle g}\uparrow & \nearrow_{\exists\, h} & \uparrow \\ A & \xrightarrow{\phi} & B * T, \end{array}$$

where ϕ is defined by $\phi(a) := (g(a), Da)$. By hypothesis, the factoring h exists. Write $h(b) = (b, D'b)$, for a k-derivation $D' : B \to T$. We have $D = D' \circ g$.

We can write $D' = \phi' \circ d_{B/k}$, for a unique B-linear map $\phi; : \Omega_{B/k} \to T$.

Now in the above diagram, take $T = \Omega_{A/k} \otimes_A B$ and $D = d_{A/k} \otimes 1$. Then the map ϕ' we get is a B-linear map $\phi' : \Omega_{B/k} \to \Omega_{A/k} \otimes_A B$, and the equality $D = D' \circ g$ implies that $d_{A/k} \otimes 1 = \phi' \circ d_{B/k} \circ g$, and thus $\phi' \circ \alpha = id_{\Omega_{A/k} \otimes_A B}$. Therefore the sequence splits. □

25. Lecture 25

25.1. The Second Fundamental Exact Sequence.

Theorem 25.1.1. *Consider a diagram $k \xrightarrow{f} A \xrightarrow{g} B = A/J$, where g is surjective and $J = \ker(g)$. Then we have:*

(1) *The following sequence is exact*

$$J/J^2 \xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \longrightarrow 0, \tag{25.1.1}$$

where $\delta(\overline{x}) = d_{A/k}(x) \otimes 1$, and α is defined as in the First Fundamental Sequence.

(2) *If B is 0-smooth over k, then*

$$0 \longrightarrow J/J^2 \longrightarrow \Omega_{A/k} \otimes_A B \longrightarrow \Omega_{B/k} \longrightarrow 0 \tag{25.1.2}$$

is split exact.

Proof. (1): For $T \in B$-Mod, consider the diagram

$$\mathrm{Hom}_B(J/J^2, T) \xleftarrow{\delta^*} \mathrm{Der}_k(A,T) \xleftarrow{\alpha^*} \mathrm{Der}_k(B,T) \longleftarrow 0.$$

Note that δ^* is simply the "restriction to J" map. So $\delta^*(D) = 0$ iff D vanishes on J iff D comes from $\mathrm{Der}_k(B,T)$. Hence this sequence is exact $\forall T$, and hence (1) follows.

(2): Suppose B is 0-smooth over k. Then we have the factoring map s in the diagram

$$\begin{array}{ccc} B & \xrightarrow{id} & B \\ \uparrow & \nearrow_{s} & \uparrow{\scriptstyle \overline{g}} \\ k & \longrightarrow & A/J^2. \end{array}$$

Thus, s gives a splitting in k-Mod of the exact sequence

$$0 \longrightarrow J/J^2 \longrightarrow A/J^2 \xrightarrow{\overline{g}} B \longrightarrow 0.$$

Now $s\overline{g} : A/J^2 \to A/J^2$ is a k-algebra homomorphism, trivial on J/J^2, and $\overline{g}(\mathrm{id} - s\overline{g}) = 0$.

Hence (by Lemma 23.3.2), $D := \mathrm{id} - s\overline{g} : A/J^2 \to J/J^2$ is a k-derivation.

Now fix $T \in B$-Mod as in the proof of (1). We want to show δ^* is surjective by constructing a section of δ^*. In fact, the map taking $\psi \in \mathrm{Hom}_B(J/J^2, T)$ to the composition D'

$$A \longrightarrow A/J^2 \xrightarrow{D} J/J^2 \xrightarrow{\psi} T$$

is such a section: if $x \in J$, and $\overline{x} \equiv x \bmod J^2$, then

$$\delta^* D'(\overline{x}) = \psi D(\overline{x}) = \psi(\overline{x} - s\overline{g}(\overline{x})) = \psi(\overline{x}).$$

Taking $T = J/J^2$ now, we see the sequence in (2) is split exact. □

Example: Let $A = k[X_1, \ldots, X_n]$, and $B = k[X_1, \ldots, X_n]/(f_1, \ldots, f_m) = k[x_1, \ldots, x_n]$. Then

$$\begin{aligned} \Omega_{B/k} &= (\Omega_{A/k} \otimes_A B)/\sum_i B\ df_i \\ &= F/R, \end{aligned}$$

where F is the free B-module with basis $dX_1, \ldots, dX_n$, and R is the B-submodule generated by $df_i = \sum_j \frac{\partial f_i}{\partial X_j}\ dX_j$.

For instance, if k is a field with $\mathrm{char}(k) \neq 2$, then for $B = k[X,Y]/(X^2 + Y^2) = k[x,y]$ we have

$$\Omega_{B/k} = B dx + B dy,$$

where the only relation is $x dx + y dy = 0$.

If $\mathrm{char}(k) = 2$, then $\Omega_{B/k} \cong B^2$.

25.2. **On tangent spaces and cotangent spaces.** Next, we want to flesh out the analogy with differential geometry. We start by defining the tangent and cotangent spaces to a variety (or scheme) at a closed point. Then we discuss vector fields.

Let $k = \overline{k}$ be an algebraically closed field. Let X be a k-variety, or more generally a finite-type separated scheme over k (to be more concrete, for our purposes, we will assume $X = \mathrm{Spec}(A)$, where A is a f.g. k-algebra. However, we will use notation that indicates that everything holds also in the non-affine case). We don't need to assume A is reduced or a domain for this discussion to be valid. By Hilbert's Nullstellensatz, a closed point $x \in X$ corresponds to a maximal ideal $m_x \subset A$. In fact, we have

$$\begin{aligned} x \in X \text{ closed point} &\longleftrightarrow \mathfrak{m}_x \in \mathrm{Spec}(A) \\ &\longleftrightarrow k\text{-alg. map } x : A \to k \\ &\longleftrightarrow k\text{-alg. map } x : \mathcal{O}_x \to k. \end{aligned}$$

In the last line, $\mathcal{O}_x$ denotes the stalk at x of the structure sheaf $\mathcal{O}_X$. Recall that the sheaf $\mathcal{O}_X$ on X has global sections $\mathcal{O}_X(X) = A$, in a canonical way. The stalk $\mathcal{O}_x$ can be identified with the localization $A_{\mathfrak{m}_x}$.

Now apply the second fundamental exact sequence to $k \longrightarrow \mathcal{O}_x \xrightarrow{x} k$. Since the composition of these maps is the identity, we find that the second fundamental sequence gives a canonical isomorphism

$$\mathfrak{m}_x/\mathfrak{m}_x^2 = \Omega_{\mathcal{O}_x/k} \otimes_{\mathcal{O}_x} k.$$

We call $\mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$ the **tangent space** of X at the point x. We call the dual k-vector space $\Omega_{\mathcal{O}_x/k} \otimes_{\mathcal{O}_x} k$, the **cotangent space** of X at x. Note that the tangent space is also the k-vector space $\mathrm{Der}_k(\mathcal{O}_x, k)$:

$$\begin{aligned}\mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k) &= \mathrm{Hom}_{\mathcal{O}_x}(\Omega_{\mathcal{O}_x/k}, k)\\ &= \mathrm{Der}_k(\mathcal{O}_x, k).\end{aligned}$$

Note also that by using a problem in Homework 2, we can identify the cotangent space as

$$\Omega_{\mathcal{O}_x/k} \otimes_{\mathcal{O}_x} k = \Omega_{A/k}/\mathfrak{m}_x\Omega_{A/k}.$$

Exercise 25.2.1. *Assume $k = \overline{k}$. Let $Y = V(f_1, \ldots, f_t) \subset \mathbb{A}_k^n$ denote a closed irreducible subset. Let $P = (P_1, \ldots, P_n)$ denote a closed point which lies in Y; denote the maximal ideals corresponding to P by $\mathfrak{a}_P = (X_1 - P_1, \ldots, X_n - P_n)$, and $\mathfrak{m} = \overline{\mathfrak{a}_P} \subset A := k[X_1, \ldots, X_n]/(f_1, \ldots, f_t)$. Show that $\mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$, the tangent space Y at P, can be identified with the kernel of $J(P) = \left[\frac{\partial f_i}{\partial X_j}(P)\right]_{ij}$, where this $t \times N$ matrix is viewed as a k-linear map $k^N \to k^t$.*

Here is another important way to think about the tangent space. Recall that in differential geometry, a tangent vector at a point x is an equivalence class of germs of curves going through x. In algebraic geometry, the role of equivalence class of curve is played by a map of k-schemes $\mathrm{Spec}(k[\epsilon]/(\epsilon^2)) \to X$. Saying it "goes through x" means the following. Denote $\Lambda := k[\epsilon]/(\epsilon^2)$, and consider the canonical k-algebra homomorphism $p : \Lambda \to k$ defined by $\epsilon \mapsto 0$. Then a map $f^* : \mathrm{Spec}(\Lambda) \to X$ is given by a k-algebra homomorphism $f : \mathcal{O}_x \to \Lambda$. It turns out that saying f^* "goes through x" is the same as saying that $pf = x$, as maps $\mathcal{O}_x \to k$. In fact, we have the following result making this precise.

Lemma 25.2.2. *There is a canonical bijection*

$$\{k\text{-alg. maps } f : \mathcal{O}_x \to \Lambda \mid pf = x\} = \mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k).$$

Proof. Consider the exact sequence

$$0 \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow \mathcal{O}_x/\mathfrak{m}_x^2 \longrightarrow \mathcal{O}_x/\mathfrak{m}_x \longrightarrow 0.$$

The map $x : \mathcal{O}_x/\mathfrak{m}_x \xrightarrow{\sim} k \hookrightarrow \mathcal{O}_x/\mathfrak{m}_x^2$ gives a splitting of the above exact sequence, and thus an identification (which depends on $x : \mathcal{O}_x \to k$) of k-algebras

$$\mathcal{O}_x/\mathfrak{m}_x^2 = \mathcal{O}_x/\mathfrak{m}_x * \mathfrak{m}_x/\mathfrak{m}_x^2.$$

We also have a canonical identification

$$\Lambda = k * k\overline{\epsilon}.$$

Note that any k-algebra homomorphism $f : \mathcal{O}_x \to \Lambda$ such that $pf = x$ necessarily takes $\mathfrak{m}_x$ into $k\overline{\epsilon}$, hence factors through $\mathcal{O}_x/\mathfrak{m}_x^2$, and is uniquely determined by its restriction to $\mathfrak{m}_x/\mathfrak{m}_x^2$. Thus giving such a homomorphism f is the same as giving a k-linear map $\mathfrak{m}_x/\mathfrak{m}_x^2 \to k\overline{\epsilon}$, in other words, an element of $\mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$. □

25.3. **Vector fields.** We push the differential geometry analogy a little further by defining vector fields. In differential geometry, a vector field is a rule assigning to each point x an element in the tangent space at x. We thus want to define "something" that gives us, for each closed point $x \in X$, a derivation in $\mathrm{Der}_k(\mathcal{O}_x, k)$. We call any element $\mathbf{D} \in \mathrm{Der}_k(\mathcal{O}_X, \mathcal{O}_X)$, a **vector field**. We claim it gives rise to $\mathbf{D}_x \in \mathrm{Der}_k(\mathcal{O}_x, \mathcal{O}_x)$, for each $x \in X$. Indeed, $\mathbf{D}$ determines a family of k-derivations

$$\mathbf{D}(U) : \mathcal{O}_X(U) \to \mathcal{O}_X(U),$$

for U ranging over the open subsets of X which contain x. Taking direct limits, we get a k-derivation

$$\mathbf{D}_x : \mathcal{O}_x \to \mathcal{O}_x.$$

Now viewing $x \in X$ as the k-algebra homomorphism $x : \mathcal{O}_x \to k$, $\mathbf{D}$ then determines a k-derivation $x \circ \mathbf{D}_x \in \mathrm{Der}_k(\mathcal{O}_x, k)$, for each x. Thus, $\mathbf{D}$ really deserves to be called a "vector field".

Fix a tangent vector $t \in \mathrm{Der}_k(\mathcal{O}_x, k)$. We say **$\mathbf{D}$ takes value t at x** if $x \circ \mathbf{D}_x = t$.

Notation: if $f \in \mathcal{O}_x$, its image $x(f) \in \mathcal{O}_x/\mathfrak{m}_x = k$ is often denoted by $f(x)$. Note that if $X = \mathrm{Spec}(A)$ and $\mathbf{D} \in \mathrm{Der}_k(A, A)$, $f \in A$, we have the formula

$$x \circ \mathbf{D}_x(f) = \mathbf{D}(f)(x).$$

25.4. **A vector field criterion for regularity.** In the following statement, X is any finite-type separated k-scheme. Since the statement is local around x, we might as well assume $X = \mathrm{Spec}(A)$ where A is a finitely-generated k-algebra, and x corresponds to the maximal ideal $\mathfrak{m}_x \subset A$.

Proposition 25.4.1. *Suppose* $\mathrm{char}(k) = 0$. *Let $x \in X$ be a closed point. Suppose that X has $n = \dim_k \mathfrak{m}_x/\mathfrak{m}_x^2$ vector fields which are linearly independent at x (meaning that the values they take at x are linearly independent tangent vectors). Then x is a regular point of X, i.e., $\mathcal{O}_x$ is a regular local ring.*

Proof. Here we give a sketch of the proof, leaving you to fill in the details.

Let $x_1, \ldots, x_n$ be elements of $\mathfrak{m}_x$ whose images give a k-basis for $\mathfrak{m}_x/\mathfrak{m}_x^2$. WLOG there are derivations $D_1, \ldots, D_n \in \mathrm{Der}_k(\mathcal{O}_x, \mathcal{O}_x)$ such that

$$D_i(x_j)(x) = \delta_{ij},$$

in other words,

$$D_i(x_j) \equiv \delta_{ij} \bmod \mathfrak{m}_x.$$

For each $p \geq 1$, we clearly have $D_i(\mathfrak{m}_x^p) \subset \mathfrak{m}_x^{p-1}$, and hence D_i extends by continuity to give a uniquely determined k-derivation $D_i \in \mathrm{Der}_k(\widehat{\mathcal{O}}_x, \widehat{\mathcal{O}}_x)$, where $\widehat{\mathcal{O}}_x$ denotes the $\mathfrak{m}_x$-adic completion of $\mathcal{O}_x$.

Define a k-algebra homomorphism $\alpha : k[[t_1, \ldots, t_n]] \to \widehat{\mathcal{O}}_x$ by $t_i \mapsto x_i$.

Define $\beta : \widehat{\mathcal{O}}_x \to k[[t_1, \ldots, t_n]]$ by

$$\beta(f) = \sum_{\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{Z}^n_{\geq 0}} \frac{(D^\nu f)(x)}{\nu!}\ t^\nu,$$

where by definition $D^\nu := D_1^{\nu_1} \circ \cdots \circ D_n^{\nu_n}$, $\nu := \nu_1! \cdots \nu_n!$, and $t^\nu := t_1^{\nu_1} \cdots t_n^{\nu_n}$.

Leibniz' rule (or rather, the generalized form $D^m fg = \sum_{k=0}^m \binom{m}{k} D^k f\, D^{m-k} g$) and an argument by induction on n shows that β is a continuous k-algebra homomorphism.

Now α is surjective since its image contains the x_i's and $\widehat{O}_x$ is complete. Since $\beta(x_i) \equiv t_i \bmod (t_1, \ldots, t_n)^2$, the elements $\beta(x_i)$ generate the ideal $(t_1, \ldots, t_n)$, and hence β is also surjective. For both cases, use Lemma 18.2.2.

Then the composition $\beta \circ \alpha$ is a surjective ring endomorphism of the Noetherian ring $k[[t_1, \ldots, t_n]]$, hence is an automorphism. Thus α is an isomorphism, and this shows $\widehat{\mathcal{O}}_x$ is a regular local ring. It follows that $\mathcal{O}_x$ is also regular. □

26. Lecture 26

26.1. **Application of vector field criterion for regularity: group schemes.** A good reference for group schemes and Hopf algebras is W.C. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag, 1979.

Let k be any field, and assume A is a f.g. k-algebra. Suppose $G = \mathrm{Spec}(A)$ is a k-**group scheme**. This is the same thing as saying that A is k-**Hopf algebra**. By definition this means that there are **comultiplication**, **counit**, and **coinverse** homomorphisms

$$\Delta : A \to A \otimes_k A$$
$$\varepsilon : A \to k$$
$$S : A \to A$$

which are compatible in a certain sense with each other (you can recover the compatibilities – certain commutative diagrams – by writing down the commutative diagrams encapsulating the group axioms for G, and then taking the "dual" commutative diagrams with respect to the anti-equivalence of categories $A \leftrightarrow \mathrm{Spec}(A)$).

The following is an important application of the vector-field criterion for regularity, Proposition 25.4.1.

Theorem 26.1.1. *If* $\mathrm{char}(k) = 0$*, then any* k*-Hopf algebra* A *is a regular ring (that is, each localization* $A_{\mathfrak{m}}$ *is regular, where* $\mathfrak{m}$ *ranges over all maximal ideals* $\mathfrak{m} \subset A$*). Thus, any* k*-group scheme is regular, and hence is reduced and non-singular as a variety.*

This is far from true when $\mathrm{char}(k) = p > 0$. Indeed, the ring $A = \mathbb{F}_p[X]/(X^p)$ is a Hopf-algebra over $\mathbb{F}_p$ whose corresponding group scheme $\mathrm{Spec}(A)$ is the group subscheme $\alpha_p \subset \mathbb{G}_a$ whose R-points for a $\mathbb{F}_p$-algebra R is the additive group $\{r \in R \mid r^p = 0\}$. Note that the ring A is not even reduced here.

Proof. For simplicity, let us assume $k = \overline{k}$. For any closed point $x \in G$, we want to check that the local ring $\mathcal{O}_x$ is regular. By translating x back to the origin $e \in G$ using the group action, it is enough to check this for $x = e$. To apply Proposition 25.4.1, we need to check that there are $\dim_k(\mathfrak{m}_e/\mathfrak{m}_e^2)$ vector fields defined near e which give a linearly independent set of values at e. To construct these vector fields, the key fact about Hopf algebras we use is that there is an isomorphism

$$\Omega_{A/k} \cong A \otimes_k \mathfrak{m}_e/\mathfrak{m}_e^2.$$

(See Theorem 11.3 in Waterhouse.) Using this, we see that

$$\begin{aligned} \mathrm{Der}_k(A, A) &= \mathrm{Hom}_A(\Omega_{A/k}, A) \\ &= \mathrm{Hom}_A(A \otimes_k \mathfrak{m}_e/\mathfrak{m}_e^2, A) \\ &= \mathrm{Hom}_k(\mathfrak{m}_e/\mathfrak{m}_e^2, A). \end{aligned}$$

Now composing the derivations with the homomorphism $e : A \to k$ shows that the derivations on the LHS take as values at e precisely the set

$$\mathrm{Hom}_k(\mathfrak{m}_e/\mathfrak{m}_e^2, k),$$

which is what we wanted to prove. □

26.2. **Separability: various notions.** Let k be a field, and A a k-algebra. We say A is **separable over** k if for every extension field $k' \supset k$, the ring $A' := A \otimes_k k'$ is reduced.
Facts (easy exercises):

- Any subalgebra of a separable algebra is separable.
- A is separable iff every f.g. k-subalgebra of A is separable.
- $A \otimes_k k'$ is reduced for every f.g. extension field $k' \supset k \implies A$ is separable.
- A is separable over $k \implies A \otimes_k k'$ is separable over k'.

We want to better understand this notion of separable, when A is finite-dimensional. So, assume $\dim_k(A) < \infty$, and fix a k-basis $\omega_1, \ldots, \omega_n$ for A. Define the **discriminant**

$$\mathrm{disc}_{A/k} = \det[\mathrm{tr}(\omega_i \omega_j)].$$

[For $a \in A$, recall that $\mathrm{tr}(a)$ is the trace of the k-linear map $A \to A$ given by multiplication by a.] Note that $d := \mathrm{disc}_{A/k}$ is a well-defined element of $k/(k^\times)^2$: If $\omega_1', \ldots, \omega_n'$ is another k-basis, write $\omega_l' = \sum_i c_{li}\, \omega_i$, and note that

$$\det[\mathrm{tr}(\omega_i' \omega_j')] = \det(c_{ij})^2 \det[\mathrm{tr}(\omega_i \omega_j)].$$

Proposition 26.2.1. *A is separable over k iff $d \neq 0$.*

Proof. ($\Leftarrow$): Let $k' \supset k$ and $A' = A \otimes_k k'$. Suppose $N := \mathrm{rad}(A') \neq 0$. Let $\omega_1, \ldots, \omega_n$ be a k'-base for A' such that $\omega_1, \ldots, \omega_r$ is a k'-base for N. Since every element of N is nilpotent, we see that $\omega_i \omega_j$ is nilpotent for i or $j \leq r$. This implies that $\mathrm{tr}(\omega_i \omega_j) = 0$ for such i, j. Hence $d = \det[\mathrm{tr}(\omega_i \omega_j)] = 0$.
($\Rightarrow$): Let K denote an algebraic closure of k. The ring $A \otimes_k K$ is reduced and Artinian, so if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the prime (= maximal) ideals of $A \otimes_k K$, we get

$$A \otimes_k K = A \otimes_k K / \cap_i \mathfrak{p}_i = \prod_i A \otimes_k K/\mathfrak{p}_i.$$

Since $A \otimes_k K/\mathfrak{p}_i$ is a finite field extension of K, it is $\cong K$, and so $A \otimes_k K \cong K^n$. Choose a basis of idempotents e_i, so that $e_i e_j = \delta_{ij}$. Then $d = \det[\mathrm{tr}(e_i e_j)] = 1 \neq 0$. □

Now change notation: assume $A := K$ is a field extension of k. Suppose K/k is an *algebraic extension* (that is, an integral extension). Recall what it means to say $\alpha \in K$ is **separable in the usual sense** over k: this is the case iff the minimal polynomial $f \in k[X]$ which α satisfies has $(f, f') = 1$. If α is not separable in the usual sense, then it is easy to see that $\mathrm{char}(k) = p > 0$, and $f(X) = g(X^p)$, for some polynomial $g \in k[X]$.

Proposition 26.2.2. *Suppose K/k is an algebraic field extension. Then K/k is separable in the usual sense $\Leftrightarrow$ it is separable.*

Proof. ($\Leftarrow$): If K/k is not separable in the usual sense, then $\exists\, \alpha \in K$ such that the minimal polynomial $f \in k[X]$ of α has $(f, f') \neq 1$. In particular, f does not have distinct roots in $k' = \overline{k}$, and the subalgebra $k(\alpha) \subset K$ has

$$k(\alpha) \otimes_k k' = k'[X]/(f),$$

a ring with non-zero nilpotents. Hence K/k is not separable.
($\Rightarrow$): Assume K/k is separable in the usual sense. WLOG K is f.g. as a field extension over k; being algebraic, this means it is f.g. as a k-algebra, hence is a finite extension of k. Then, since K/k is separable in the usual sense and is now also finite, $K = k(\theta)$, for some $\theta \in K$. Let $f \in k[X]$ be the minimal polynomial of θ. Let $k' \supset k$, and factor f in $k'[X]$ as

$$f = f_1 \cdots f_r,$$

where the f_i are *distinct* irreducible elements of $k'[X]$. By the Chinese remainder theorem,

$$K \otimes_k k' = k'[X]/(f) = \prod_{i=1}^{r} k'[X]/(f_i).$$

This is a product of fields, hence is reduced. This shows that K/k is separable. □

We say a field extension K/k is **separably generated** if K has a transcendence basis Γ such that $K/k(\Gamma)$ is a separable algebraic extension.

Lemma 26.2.3. *Any separably generated extension is separable.*

Proof. Suppose Γ is the aforementioned transcendence basis. Let $k' \supset k$ be any field extension.

The natural map $k(\Gamma) \otimes_k k' \to k'(\Gamma)$ is an isomorphism (this follows easily, using that it restricts to give the obvious isomorphism $k[\Gamma] \otimes_k k' \xrightarrow{\sim} k'[\Gamma]$).

Thus $K \otimes_k k' = K \otimes_{k(\Gamma)} (k(\Gamma) \otimes_k k') = K \otimes_{k(\Gamma)} k'(\Gamma)$. Since $K/k(\Gamma)$ is separable, the latter is reduced, and thus so is $K \otimes_k k'$. □

For the next proposition, assume $\mathrm{char}(k) = p > 0$, and define $k^{1/p} := \{x \in \overline{k} \mid x^p \in k\}$. Note that $k^{1/p}$ is an extension field of k.

Proposition 26.2.4. *Suppose* $\mathrm{char}(k) = p$*, and K is a f.g. extension field of k. Then TFAE:*

(1) *K is separable over k.*
(2) *$K \otimes_k k^{1/p}$ is reduced.*
(3) *K is separably generated over k.*

Proof. The implication (1) $\Rightarrow$ (2) is trivial, and in the above lemma we proved the implication (3) $\Rightarrow$ (1).

Let us prove (2) $\Rightarrow$ (3). Write $K = k(x_1, \ldots, x_n)$. WLOG $x_1, \ldots, x_r$ comprise a transcendence basis for K/k. Let's assume that $k(x_1, \ldots, x_r, \ldots, x_q)$ is separable over $k(x_1, \ldots, x_r)$, but $y = x_{q+1}$ is not separable over $k(x_1, \ldots, x_r)$.

Let $f(Y^p)$ be the minimal polynomial of y over $k(x_1, \ldots, x_r)$. Clearing denominators, get an irreducible polynomial $F(X_1, \ldots, X_r, Y^p)$ with $F(x, y^p) = 0$.

If $\partial F/\partial X_i = 0$ for all $1 \leq i \leq r$, then $F(X, Y^p) = G(X, Y)^p$, for some $G(X, Y) \in k^{1/p}[X, Y]$. But then $k[x_1, \ldots, x_r, y] \otimes_k k^{1/p} = k[X, Y]/(F(X, Y^p)) \otimes_k k^{1/p}$, which is also $k^{1/p}[X, Y]/(G(X, Y)^p) \subset K \otimes_k k^{1/p}$. So $K \otimes_k k^{1/p}$ is not reduced.

Therefore, we can assume WLOG that $\partial F/\partial X_1 \neq 0$. Then x_1 is separable algebraic over $k(x_2, \ldots, x_r, y)$, hence so are the elements $x_{r+1}, \ldots, x_q$ (check this!). Thus, exchanging $x_1 \leftrightarrow y = x_{q+1}$, we find $x_{r+1}, \ldots, x_{q+1}$ are separable algebraic over $k(x_1, \ldots, x_r)$. So by induction on q, we conclude that, after possibly rearranging and relabeling the elements $x_1, \ldots, x_n$ repeatedly, K is separable algebraic over $k(x_1, \ldots, x_r)$, as desired. □

26.3. **Perfect fields.** We say a field k is **perfect** if every algebraic extension K/k is separable. For example, every characteristic zero field is perfect, since K/k is clearly separable in the usual sense.

Lemma 26.3.1. *If k is perfect then*

(1) *every extension K/k is separable;*
(2) *a k-algebra is separable iff it is reduced.*

Proof. (1): If $\mathrm{char}(k) = 0$, then K/k is separably generated (once one checks it has a transcendence basis), and thus separable. If $\mathrm{char}(k) = p$, then $k = k^{1/p}$: note that if $k^{1/p} \neq k$, then $k^{1/p}$ is an algebraic extension of k which is not separable in the usual sense (check!).

From $k = k^{1/p}$ it follows from the preceding proposition that every f.g. subextension of K/k is separable. Hence K/k is separable.
(2): We need to show that if A is a reduced k-algebra, then it is separable (the converse being immediate). WLOG A is f.g. over k, so is Noetherian and reduced. In that case, the exercise below asserts that the **total ring of fractions of** A, namely the localization $\Phi A := S^{-1}A$ where S is the set of all non-zero divisors in A, is a product of fields. Write $\Phi A = K_1 \times \cdots \times K_r$. Each K_i/k is separable by (1), and so ΦA is also separable. Since $A \subset \Phi A$, we see A is separable as well. □

Exercise 26.3.2. *Show that is A is a reduced Noetherian ring, then the total ring of fractions ΦA is a product of fields.*

Exercise 26.3.3. *Suppose k has $\mathrm{char}(k) = p$ and $k^{1/p} = k$. Show that k is perfect. Thus, perfect fields are precisely those satisfying one of the following two properties:*

(1) $\mathrm{char}(k) = 0$, *or*
(2) $\mathrm{char}(k) = p$ *and* $k^{1/p} = k$.

Remark 26.3.4. *Are non-perfect fields important? Yes, they arise very naturally, especially in algebraic geometry and number theory. For example, the non-Archimedean local field $\mathbb{F}_p((t))$ is non-perfect, as is the global function field $\mathbb{F}_p(t)$ (= the field of "meromorphic" functions on the curve $\mathbb{P}^1$ over the field $\mathbb{F}_p$).*

27. Lecture 27

27.1. **Regularity via the structure of $\Omega_{B/k}$.** Let K/k be a f.g. extension of fields. In the following subsection we will prove that

$$\dim_K \Omega_{K/k} \geq \mathrm{tr.deg}_k K \tag{27.1.1}$$

with equality iff K/k is separably generated (we will actually prove something more general). Let us assume this for now, and derive some consequeces.

In this subsection, we assume B is the localization at a maximal ideal $\mathfrak{m}$ of a f.g. k-algebra A. In the next statement, we use the symbol $\mathfrak{m}$ also to denote the maximal ideal of the local ring B. The proof is deferred to the next lecture.

Proposition 27.1.1. *Assume k is perfect and that $A/\mathfrak{m} = k$ (e.g. k could be any algebraically closed field). The local ring $(B, \mathfrak{m})$ is regular iff $\Omega_{B/k}$ is a free B-module of rank $\dim(B)$.*

Why is this important? Returning to our algebra A above, which we now assume is a domain, we can now prove that $A_{\mathfrak{m}}$ is regular, for "generic" $\mathfrak{m}$. Let $K := \mathrm{Frac}(B) = \mathrm{Frac}(A)$; this is a f.g. field extension of k.

Theorem 27.1.2 (Comp. Hartshorne, II Cor. 8.16, and Exercise 22.2.3 of these notes.)**.** *Assume $k = \overline{k}$. Let X be an irreducible variety over k (ie a finite-type, separated, reduced and irreducible k-scheme). Then there is an open dense set of X which is non-singular.*

Proof. Because non-singularity is a local property, we may assume $X = \mathrm{Spec}(A)$, where A is a k-algebra and a domain. We need to find a non-empty open subset $D(f) \subset X$ such that for each maximal ideal $\mathfrak{m} \in D(f)$, the local ring $A_{\mathfrak{m}}$ is regular. By the proposition above, this amounts to showing that for such $\mathfrak{m}$'s, the $A_{\mathfrak{m}}$-module $\Omega_{A_{\mathfrak{m}}/k} = \Omega_{A/k} \otimes_A A_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module of rank $\dim(A_{\mathfrak{m}}) = \dim(A) = \mathrm{tr.deg}_k(A)$ (we used Theorem 7.3.1 for these last equalities). Let us write $M = \Omega_{A/k}$; the equality $M_{\mathfrak{m}} = \Omega_{A_{\mathfrak{m}}/k}$ cited above is a consequence of the general equality

$$\Omega_{S^{-1}C/A} = \Omega_{C/A} \otimes_C S^{-1}C$$

for an A-algebra C, assigned in Homework 2.

Let $K = \mathrm{Frac}(A)$. Now, since $k = \overline{k}$ is perfect, the extension K/k is automatically separably generated, and hence by (27.1.1) we have $\dim_K \Omega_{K/k} = \dim(A)$. Also, by the Homework exercise just cited above, we have $\Omega_{K/k} = M \otimes_A K$.

Now we apply the following general argument to complete the proof that $A_{\mathfrak{m}}$ is generically regular, which completes the proof of the Theorem. □

Lemma 27.1.3. *Let A be a Noetherian domain, with fraction field K and let M be a f.g. A-module. Assume that $M \otimes_A K = K^n$. Then there exists $f \in A - 0$ such that $M_f = M \otimes_A A_f \cong A_f^n$. Thus, for $\mathfrak{m} \in D(f)$, we have $M_{\mathfrak{m}} \cong A_m^n$.*

Proof. We may choose a K-basis of $M_K := M \otimes_A K$ having the form $x_1 \otimes 1, \ldots, x_n \otimes 1$, where all $x_i \in M$. Sending $e_i \mapsto x_i$ defines an A-module map $A^n \to M$ which becomes an isomorphism upon tensoring with K. Consider the exact sequence

$$0 \to \mathrm{Ker} \to A^n \to M \to \mathrm{Cok} \to 0.$$

The A-modules Ker and Cok are f.g., and have $\mathrm{Ker}_K = \mathrm{Cok}_K = 0$. Hence there exists $f \in A - 0$ which annihilates both Ker and Cok. This f has the required properties. □

27.2. **Relating $\Omega_{L/k}$ and $\Omega_{K/k}$.** Consider the following general set-up: $L \supset K \supset k$ are field extensions, and L/K is a f.g. field extension. Define $r(L) = \dim_L \Omega_{L/k}$ and $r(K) = \dim_K \Omega_{K/k}$. We want to find the relation between the numbers $r(L)$ and $r(K)$.

By induction, we reduce to the case $L = K(t)$, where $t \in L$. Then there are essentially four cases to consider:

-(1) t is transcendental over K.
-(2) t is a separable algebraic element.
-(3) $L = K[X]/(X^p - a)$, where $a \in K$ and $d_{K/k}a = 0$.
-(4) L as above, but $d_{K/k}a \neq 0$.

Case (1): For psychological reasons, write $t = X$. Then since $K[X]/K$ is 0-smooth (check this!), the first fundamental sequence for $k \to K \to K[X]$ is split exact. Thus,

$$\Omega_{K[X]/k} = (\Omega_{K/k} \otimes_K K[X]) \ \oplus \ \Omega_{K[X]/K}.$$

Applying $- \otimes_{K[X]} L$ and recalling $\Omega_{K[X]/K} = K[X]\, dX$, we see

$$\Omega_{L/k} = (\Omega_{K/k} \otimes_K L) \ \oplus \ L\, dX,$$

and thus $r(L) = r(K) + 1$.

Case (2): We will prove in the lemma below that L/K is 0-étale, and hence the first fundamental sequcence associated to $k \to K \to L$ is split exact, and moreover the third member has $\Omega_{L/K} = 0$ (since L/k is 0-unramified). Thus we see $\Omega_{L/k} = \Omega_{K/k} \otimes_K L$, and so $r(L) = r(K)$.

Lemma 27.2.1. *If L/K is a separable algebraic extension, it is* 0*-étale.*

Proof. It is not hard to reduce to the case where L/K is a finite separable extension (by uniqueness the tower of lifts glue to define one on L), which is all we need in Case 2 anyway.

Write $L = K(\alpha)$, where α has minimal polynomial $f \in K[X]$. So $L = K[X]/(f)$. Consider a diagram

$$\begin{array}{ccc} L & \xrightarrow{u} & C/J \\ \uparrow & \overset{v}{\searrow} & \uparrow \\ K & \longrightarrow & C \end{array}$$

where $J \subset C$ is an ideal such that $J^2 = 0$, and the map u is given such that the square commutes. We want to show that a unique v exists making the triangles commute.

Existence of v: It's enough to find an element $y \in C$ such that $f(y) = 0$ and $y \bmod J = u(\alpha)$; then we can define v by sending the image of X in L to $y \in C$.

To find y, let $y' \in C$ be any lift of $u(\alpha)$. Note that $f(y') \in J$, since the image of $f(y')$ in C/J is $f(u(\alpha)) = 0$. Since $J^2 = 0$, for any $\eta \in J$ we have

$$f(y' + \eta) = f(y') + f'(y')\eta.$$

As $f'(\alpha) \in L^\times$ (since $(f, f') = 1$), we see that $f'(y') \in C^\times$. Then by taking

$$\eta := -\frac{f(y')}{f'(y')},$$

an element of J, we get $f(y' + \eta) = 0$. So we can set $y = y' + \eta$.

Uniqueness of v: If $y, y + \eta$ are two lifts in C of $u(\alpha) \in C/J$, then $\eta \in J$, and we have

$$f(y + \eta) = f(y) + f'(y)\eta.$$

If in addition we have $f(y+\eta) = f(y) = 0$, then because $f'(y) \in C^\times$, we must have $\eta = 0$. This shows that v is unique, proving the lemma. □

For the remaining two cases, we may assume L/K is a purely inseparable extension of form $L = K[X]/(X^p - a)$, where $a \in K$. Write $f(X) := X^p - a$.

Claim: $\Omega_{L/k} = ((\Omega_{K/k} \otimes_K L) \ \oplus \ L\, dX)/L\, \delta f$, where $\delta f := df(t) + f'(t)\, dX$.

Proof: Here, the symbol $df \in \Omega_{K/k} \otimes_K K[X]$ is the element given by applying $d_{K/k}$ to the coefficients of $f(X)$, and $df(t)$ is the "reduction modulo (f)" of that element,

i.e. its image in $\Omega_{K/k} \otimes_K L$. Also, $f'(t)$ is the "reduction modulo (f)" of $f'(X)$, so that $f'(t)\,dX \in L\,dX$.

To prove the claim, first apply the second fundamental sequence to $k \to K[X] \twoheadrightarrow L$ to get the exact sequence

$$\frac{(f)}{(f)^2} \to \Omega_{K[X]/k} \otimes_{K[X]} L \to \Omega_{L/k} \to 0, \tag{27.2.1}$$

where the first map sends $f \mapsto d_{K[X]/k} f \otimes 1$.

Also, since $K[X]/K$ is 0-smooth, the first fundamental exact sequence for $k \to K \to K[X]$ gives a split exact sequence

$$0 \to \Omega_{K/k} \otimes_K K[X] \to \Omega_{K[X]/k} \to \Omega_{K[X]/K} \to 0 \tag{27.2.2}$$

where the splitting is given by $d_{K[X]/k} g(X) \mapsto dg$, a left-inverse of the map $\Omega_{K/k} \otimes_K K[X] \to \Omega_{K[X]/k}$ (check it is a left-inverse!).

Now substituting (27.2.2) into (27.2.1) proves the claim.

Case (3): We have $\delta(X^p - a) = 0$, and so the claim shows that $\Omega_{L/k} = (\Omega_{K/k} \otimes_K L) \oplus L\,dX$, and hence $r(L) = r(K) + 1$.

Case (4): We have $\delta(X^p - a) \neq 0$, and so $r(L) = r(K)$.

In summary, we have the following formulas:

- Case (1): $r(L) = r(K) + 1$;
- Case (2): $r(L) = r(K)$;
- Case (3): $r(L) = r(K) + 1$;
- Case (4): $r(L) = r(K)$.

This immediately implies the first parts of the following theorem.

Theorem 27.2.2. *Suppose $L \supset K \supset k$ are extension of fields, and suppose L/K is a f.g. field extension. Then*

(i) $\dim_L \Omega_{L/k} \geq \dim_K \Omega_{K/k} + \text{tr.deg}_K L$;
(ii) *Equality holds if L/K is separably generated.*
(iii) *If L/k is f.g., then $\dim_L \Omega_{L/k} \geq \text{tr.deg}_k L$, and equality holds iff L/k is separably generated. In particular, $\Omega_{L/k} = 0 \Leftrightarrow L/k$ is a separable algebraic exension.*

Proof. (i,ii): By induction on the number of generators of the field extension L/K, we may assume $L = K(t)$, and then these two statements follow by a consideration of Cases (1-4) above.

(iii): Take $K = k$ to get the inequality $\geq$. Next, assume $\Omega_{L/k} = 0$. So $r(L) = 0$, and for every field K with $L \supset K \supset k$ we have $r(K) = 0$ as well. Only Case (2) above can occur for $L/K/k$, and so we see that L/k is separable and algebraic.

Next, assume $r(L) = \text{tr.deg}_k L =: r$. Choose $x_1, \ldots, x_r \in L$ such that $dx_1, \ldots, dx_r$ form an L-base of $\Omega_{L/k}$. It is easy to show that the elements $x_1, \ldots, x_r$ are algebraically independent over k.

Let $k(x) := k(x_1, \ldots, x_r) \subset L$. We claim $L/k(x)$ is separable and algebraic. The first fundamental exact sequence applied to $k \to k(x) \to L$ gives an exact sequence

$$\Omega_{k(x)/k} \otimes_{k(x)} L \to \Omega_{L/k} \to \Omega_{L/k(x)} \to 0$$

in which the left-most arrow is surjective (by choice of the x_i). Thus $\Omega_{L/k(x)} = 0$, and so by the statement proved above, $L/k(x)$ is separable algebraic, as desired. $\square$

28. Lecture 28

28.1. **Proof of Proposition 27.1.1.** Recall we have assumed k is perfect, and $B/\mathfrak{m} = k$. Note that we have *not* assumed A (or B) is a domain for this proposition.

First suppose $\Omega_{B/k}$ is a free B-module of rank $\dim(B)$. Then the second fundamental exact sequence for $k \to B \twoheadrightarrow B/\mathfrak{m}$ yields

$$\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\sim} \Omega_{B/k} \otimes_B B/\mathfrak{m}.$$

So $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \mathrm{rank}_B \Omega_{B/k} = \dim(B)$, and so B is regular.

Conversely, assume $(B, \mathfrak{m})$ is regular. Recalling that B is then automatically a domain, we set $K := \mathrm{Frac}(B)$. Using the argument above, we get from $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(B)$ that $\dim_k \Omega_{B/k} \otimes_B k = \dim(B) =: r$. Since k is perfect, the extension K/k is separably generated, and thus we have

$$\dim_K \Omega_{B/k} \otimes_B K = \mathrm{tr.deg}_k K = r.$$

Now the B-module $\Omega_{B/k}$ has

$$\dim_F \Omega_{B/k} \otimes_B F = r$$

for $F = K$ and $F = k$. It follows from this that $\Omega_{B/k} \cong B^r$, and we are done. □

We used the following general lemma (see Hartshorne, II, Lemma 8.9).

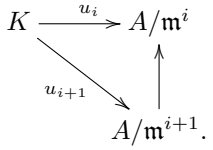
Lemma 28.1.1. *Suppose $(A, \mathfrak{m})$ is a Noetherian (this is not needed) local domain with $K := \mathrm{Frac}(A)$ and $k := A/\mathfrak{m}$. Suppose M is a f.g. A-module such that $\dim_k M \otimes_A K = \dim_k M \otimes_A k = r$. Then M is free of rank r.*

28.2. **Formal smoothness.** Here is our motivation. If $(A, \mathfrak{m}, K)$ is a local ring ($K := A/\mathfrak{m}$), then we say A has a **coefficient field** if there is a subfield $K' \subset A$ such that the composition $K' \hookrightarrow A \twoheadrightarrow K$ is an isomorphism. Obviously in order for A to have a coefficient field, it must contain *some* field. An important question goes in the opposite direction: supposing A contains some field, does it then have a coefficient field?

Theorem 28.2.1 (I.S. Cohen)**.** *If $(A, \mathfrak{m}, K)$ is a complete Noetherian local ring and A contains a field k, then A has a coefficient field. If K/k is separable, then there is a coefficient field containing k.*

Corollary 28.2.2 (Cohen Structure Theorem)**.** *If $(A, \mathfrak{m}, K)$ is a complete regular local ring containing a field, then $A \cong K[[X_1, \ldots, X_d]]$, where $d = \dim(A)$.*

Here is the idea behind the proof of the theorem (we'll give the details later). It's ETS that there is a map $u : K \to A$ such that $pu = \mathrm{id}_K$, where $p : A \to A/\mathfrak{m} = K$ is the projection. Since $A = \varprojlim A/\mathfrak{m}^i$, it's ETS that for each successive lift $u_i : K \to A/\mathfrak{m}^i$ of $u_1 = \mathrm{id}_K$, we can lift one step further, i.e. find u_{i+1} making the following commute:



If possible, we lift u_1 to get a compatible family of lifts $u_1, u_2, u_3, \ldots$, and these determine the desired map $u : K \to \varprojlim A/\mathfrak{m}^i = A$.

Thus, what is required of the map $k \to K$ (where is $k \subset A$ is the given subfield) is that it be 0-smooth. We will study a circle of ideas related to proving that in many cases K/k is 0-smooth. Along the way it is convenient to introduce a notion of smoothness wherein the topology plays a role. This notion is called *formal smoothness*.

To define it we need some preliminary definitions. Suppose A is a topological ring. We say $I \subset A$ is an **ideal of definition** if $\{I^n\}$ is a basis of open neighborhoods around $0 \in A$. We say a topological A-module M is **discrete** if $IM = (0)$ for some open ideal $I \subset A$. If A is a local or semi-local ring and $J \subset A$ is the Jacobson radical of A, unless otherwise mentioned we always give A the J-adic topology.

Suppose $g : k \to A$ is a continuous map of topological rings. We say g is **formally smooth**, or **fs**, if for every discrete ring C, and ideal $N \subset C$ with $N^2 = 0$, if we are given continuous maps u, v making the following square commute, there is a lift $v' : A \to C$ of v making the triangles commute:

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & \nearrow_{v'} & \uparrow \\ k & \xrightarrow{u} & C. \end{array}$$

Remark 28.2.3. (1) *The map v' is automatically continuous: there is an open ideal $I \subset A$ such that $v(I) = 0$. i.e. $v'(I) \subset N$ and so $v'(I^2) = 0$. Since I^2 is an open ideal, this shows that v' is continuous.*

(2) *In the definition of* **fs**, *we can replace "$N^2 = 0$" with "N is nilpotent". Indeed, suppose $N^m = 0$ and that we can perform lifting for ideals whose squares are zero. Then lift $A \to C/N$ first to $A \to C/N^2$, and then to $A \to C/N^3$. Continuing, we eventually lift to $A \to C/N^m = C$.*

(3) *If C is a complete and Hausdorff with ideal of definition N (so that $C = \varprojlim C/N^i$), then we can use the above argument to show that we can lift $v : A \to C/N$ to $A \to \varprojlim C/N^i = C$.*

If A is fs over k for the discrete topologies on k, A, then we say A is **smooth** over k. This is the same as our earlier notion of **0-smooth**.

Thus, $k \to A$ smooth implies $k \to A$ is fs for any adic topologies on k, A such that $k \to A$ is continuous.

The following lemma explains to some extent why we use the terminology "formally smooth" (since completions are connected to Grothendieck's theory of "formal schemes"). It also highlights the importance of the continuity hypotheses in the definition of formal smoothness.

Lemma 28.2.4. *Let $\widehat{A}$ denote the I-adic completion of A, a Noetherian k-algebra (where k is any ring). Then A is fs over k iff $\widehat{A}$ is fs over k.*

Proof. Suppose given a continuous $v : A \to C/N$ making the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow \\ k & \xrightarrow{u} & C. \end{array}$$

Since v is continuous, it factors through a map $\bar{v} : A/I^m \to C/N$. Clearly if $\bar{v}$ lifts to k-algebra map $\bar{v}' : A/I^m \to C$, then v lifts to a k-algebra map $v' : A \to C$. Conversely, if v lifts to v', then for some sufficiently large m, $\bar{v}$ lifts to a $\bar{v}'$. Thus, $k \to A$ is fs iff given any such diagram, for a sufficiently large m, the map $\bar{v} : A/I^m \to C/N$ lifts to a map $\bar{v}' : A/I^m \to C$.

The same argument applies to $\widehat{A} \supset \widehat{I}$ replacing $A \supset I$. Also, recall that for every integer m, $A/I^m = \widehat{A}/\widehat{I}^m$. It is now clear that A is fs over k iff $\widehat{A}$ is. □

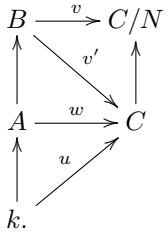
Examples

(1) $A = k[\dots, X_\lambda, \dots]$ is smooth over k, for any ring k and any family of indeterminates X_λ.
(2) If k denotes a Noetherian ring endowed with the discrete topology, then $A = k[[X_1, \dots, X_n]]$ is fs over k. (This follows from the lemma above, since A is the $(X_1, \dots, X_n)$-adic completion of the fs (even smooth) k-algebra $k[X_1, \dots, X_n]$.

28.3. **Some properties of formally smooth morphisms.** The following properties are analogous to properties of smooth morphisms in the categories of varieties or schemes.

Transitivity: If B is a fs A-algebra and A is a fs k-algebra, then B is a fs k-algebra.

Proof. Given the morphisms u, v making the outer quadrilateral commute, we first lift to find w (using A/k is fs), and then lift w to find v' (using B/A is fs).



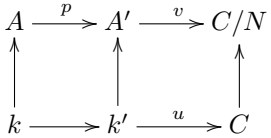
□

Localization: If $S \subset A$ is a multiplicative set, then $S^{-1}A$ is smooth over A. (In fact, we showed that $S^{-1}A$ is 0-étale over A, which is stronger.)

Base Change: Suppose k, A, k' are topological rings, and $k \to A$ and $k \to k'$ are continuous ring homomorphisms. Let $A' = A \otimes_k k'$ be endowed with the topology of the tensor product. This means that if $\{I_n\} \subset A$ and $\{J_m\} \subset k'$ are families of ideals defining the topologies on A and k', then we define the topology on A' to be the one defined by the family $\{I_n A' + J_m A'\}_{n,m}$.

If A is fs over k, then A' is fs over k'.

Proof. Let $p : A \to A'$ and $k' \to A'$ be the canonical maps; they are continuous. Given C, N, u, v in the diagram below making the rightmost square commutative



use the fs of A/k to find the lifting $w : A \to C$ of $vp : A \to C/N$. Then define $A' \to C$ by $a \otimes k' \mapsto w(a)u(k')$. This is a lift of v, as desired. □

28.4. **Separability and smoothness for field extensions.** The following fact is fundamental, and will easily imply the theorems of Cohen.

Theorem 28.4.1. *A field extension K/k is smooth iff it is separable.*

We refer to this as the **fundamental fact**.

28.5. **Proofs of Cohen's theorems, modulo the fundamental fact.** We now prove Theorem 28.2.1 and Corollary 28.2.2, modulo Theorem 28.4.1.

Proof of Theorem 28.2.1: If K/k is separable, then by the fundamental fact, K/k is smooth. Hence we can lift $\mathrm{id}_K : K \to A/\mathfrak{m}$ to a k-algebra homomorphism $K \to \varprojlim A/\mathfrak{m}^i = A$. In general, let $k_0 \subset k$ be the prime field. Then K/k_0 is separable since k_0 is perfect, hence the above argument applies to produce the coefficient field. □

Corollary 28.5.1. *Let $(A, \mathfrak{m}, K)$ be a complete Hausdorff local ring containing a field. Then if $\mathfrak{m}$ is a f.g. ideal, the ring A is Noetherian.*

Proof. Suppose $\mathfrak{m} = (x_1, \ldots, x_n)$, and let $K' \subset A$ be the coefficient field produced by Theorem 28.2.1. Sending $X_i \mapsto x_i$ defines a surjective K'-algebra homomorphism

$$K'[[X_1, \ldots, X_n]] \to A.$$

The definition makes sense since A is complete. Also, note that it is surjective on the associated graded level (check this!), and so surjective by Lemma 18.2.2. Hence A is Noetherian, being a quotient of a Noetherian ring. □

Proof of Corollary 28.2.2: Note that since $(A, \mathfrak{m}, K)$ is regular of dimension d, we have in this case $\mathfrak{m} = (x_1, \ldots, x_d)$. Now from the proof of the corollary above, we have

$$K[[X_1, \ldots, X_d]]/P = A,$$

where P is a prime ideal (recall that A is a domain, being regular). But then dimension considerations show that $P = 0$ (otherwise the LHS would have dimension $< d = \dim(A)$). We are done. □

28.6. **Formal smoothness implies regularity.**

Proposition 28.6.1. *let $(A, \mathfrak{m}, K)$ be a Noetherian local ring containing a field k. If A/k is fs, then A is regular.*

Proof. Let $k_0 \subset k$ denote the prime field. Note that k/k_0 is separable, hence smooth, hence fs. Also, A is fs over k by hypothesis. Hence by transitivity, A/k_0 is fs. Thus, WLOG k is perfect.

Let K' denote a coefficient field of the complete local ring $A/\mathfrak{m}^2$, containing k (use Theorem 28.2.1). Let $x_1, \ldots, x_d \in \mathfrak{m}$ be a set of elements whose reductions determine a K'-basis of $\mathfrak{m}/\mathfrak{m}^2$.

There is an isomorphism of k-algebras

$$v_1 : A/\mathfrak{m}^2 \xrightarrow{\sim} K'[X_1, \ldots, X_d]/J^2,$$

where $J := (X_1, \ldots, X_d)$. (To see this, use that the obvious map from the RHS to the LHS is an isomorphism on the associated graded level, hence is an isomorphism since both sides are complete.)

Define $v : A \twoheadrightarrow K'[X]/J^2$ as the composition of v_1 with the projection $A \to A/\mathfrak{m}^2$. Now, using that A/k is fs, lift v to k-algebra maps $v'_n : A \to K'[X]/J^{n+1}$, for $n = 2, 3, \ldots$.

Since the elements $v(x_1), \ldots, v(x_d)$ generate $J/J^2 = \overline{J}/\overline{J}^2$ (where $\overline{J} := J/J^{n+1}$), the elements $v'_n(x_1), \ldots, v'_n(x_d)$ generate $\overline{J}$ (by NAK).

It follows that

$$\begin{aligned} K'[X]/J^{n+1} &= v'_n(A) + \overline{J}^2 \\ &= v'_n(A) + \sum_i v'_n(x_i)(v'_n(A) + \overline{J}^2) \\ &= v'_n(A) + \overline{J}^3 \\ &= \cdots \\ &= v'_n(A) + \overline{J}^{n+1} \\ &= v'_n(A). \end{aligned}$$

Thus $v'_n : A \twoheadrightarrow K'[X]/J^{n+1}$. Therefore

$$\dim(A) = \deg \ell(A/\mathfrak{m}^{n+1}) \geq \deg \ell(K'[X]/J^{n+1}) = d.$$

Since $\mathfrak{m}$ is generated by d elements, this shows that A is regular, as desired. □

29. Lecture 29

29.1. **How liftings lead to 2-cocycles.** Here we give the first steps of our goal: a homological criterion for smoothness over a field k. This will be a key ingredient in our proof of the fundamental fact (Theorem 28.4.1).

Assume for the time being that k is a field. Consider the usual diagram

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow{\scriptstyle q} \\ k & \xrightarrow{u} & C. \end{array}$$

From this we define a k-subalgebra $E \subset A \times C$ by

$$E := \{(a, c) \mid v(a) = q(c)\}.$$

This is part of an extension of A by N:

$$0 \to N \to E \to A \to 0,$$

where $N \to E$ is $n \mapsto (0, n)$ and $E \to A$ is $(a, c) \mapsto a$. The following result is fundamental, but is easy and is left to the reader.

Lemma 29.1.1. *The map v lifts to a k-algebra map $v' : A \to C$ iff $0 \to N \to E \to A \to 0$ splits in the category of k-algebras (meaning the splitting map $A \to E$ is a k-algebra homomorphism).*

Proof. Exercise. □

Now, since k is a field, and everthing in sight is a k-vector space, the extension E always splits in the category of k-vector spaces. We may therefore write $E = A \oplus N$, and then express the multiplication in terms of a symmetric 2-cocycle

$$f : A \times A \to N.$$

That is, the multiplication in E can always be expressed as

$$(a_1, n_1) \cdot (a_2, n_2) = (a_1a_2, a_1n_2 + a_2n_1 + f(a_1, a_2)),$$

where f is symmetric, bilinear and satisfies (by associativity in E) the relation

$$af(b, c) - f(ab, c) + f(a, bc) - f(a, b)c = 0,$$

for all $a, b, c \in A$.

Such extensions are called **Hochschild extensions**. We will define this formally in the next subsection. Note that it is already clear that the splitting of the extension in the category k-Alg is detected by whether the 2-cocycle f is "trivial" or not. Thus, the smoothness of $k \to A$ is going to be related to the vanishing of a certain H^2 cohomology group.

In the next few subsections, we will explain this more formally.

29.2. **Extensions.** Here we continue to work towards a cohomological criterion for smoothness of $k \to A$, where k is a field. The same discussion goes over word-for-word when we only assume k is a ring and A is projective as a k-module.

Given a k-algebra and ideal $C \supset N$, with $N^2 = 0$, write $C' := C/N$. Then N is naturally a C'-module. Conversely, suppose C' is a ring and let N be any C'-module. An **extension of C' by N** is a triple (C, ϵ, i) such that

- C is a ring;
- $\epsilon : C \twoheadrightarrow C'$, and $\ker(\epsilon)^2 = 0$;
- $i : N \xrightarrow{\sim} \ker(\epsilon)$ is an isomorphism of C'-modules.

We represent the extension with an exact sequence

$$0 \longrightarrow N \xrightarrow{i} C \xrightarrow{\epsilon} C' \longrightarrow 0.$$

Given a C'-module N, we always have the **trivial extension** $C' * N = C' \oplus N$, where the multiplication is defined by

$$(a, x) \cdot (b, y) := (ab, ay + bx).$$

An isomorphism between (C, ϵ, i) and (C_1, ϵ_1, i_1) is a ring homomorphism $f : C \to C_1$ such that the following commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & C & \xrightarrow{\epsilon} & C' & \longrightarrow & 0 \\ & & \Big\| & & \Big\downarrow{\scriptstyle f} & & \Big\| & & \\ 0 & \longrightarrow & N & \xrightarrow{i_1} & C_1 & \xrightarrow{\epsilon_1} & C' & \longrightarrow & 0. \end{array}$$

Such an f is automatically an isomorphism (the snake lemma or the 5-lemma), and is *unique* (check this!).

Exercise 29.2.1. *Show that $(C, \epsilon, i) \cong C' * N \Leftrightarrow \exists$ a ring homomorphism section $s : C' \to C$ for ϵ such that $\epsilon \circ s = \mathrm{id}_{C'}$.*

29.3. **Hochschild extensions.** We say (C, ϵ, i) is a **Hochschild extension** if the exact sequence

$$0 \longrightarrow N \xrightarrow{i} C \xrightarrow{\epsilon} C' \longrightarrow 0$$

splits in $\mathbb{Z}$-mod: there exists an additive map $s : C' \to C$ such that $\epsilon \circ s = \mathrm{id}_{C'}$.

In that case, $C = C' \oplus N$ as an abelian group, and the multiplication in C is given by

$$(a, x) \cdot (b, y) = (ab, ay + bx + f(a, b)),$$

for a function $f : C' \times C' \to N$. Why? Write $(a, 0) = s(a)$. Note that $\epsilon(s(a)s(b) - s(ab)) = 0$ implies that the function f is given by

$$f(a, b) := s(a)s(b) - s(ab) \ \in N.$$

Note that f is symmetric (since C is commutative), bilinear, and satisfies the following cocycle relation (a rephrasing of "C is associative"):

$$af(b, c) - f(ab, c) + f(a, bc) - f(a, b)c = 0, \tag{29.3.1}$$

for $a, b, c \in C'$. Such a function $f : C' \times C' \to N$ is called a **symmetric 2-cocycle**. Without the hypothesis of symmetry, f is called simply a **2-cocycle**.

Conversely, any such f gives rise to a Hochschild extension of C' by N. The extension is isomorphic to the trivial extension $C' * N$ iff $\exists\ g : C' \to N$ such that

$$f(a, b) = ag(b) - g(ab) + g(a)b. \tag{29.3.2}$$

In this case we say f is a **2-coboundary**. More generally, two Hochschild extensions determined by $f_1, f_2 : C' \times C' \to N$ are isomorphism iff $f_1 - f_2$ is a 2-coboundary (check this!).

The quotient of symmetric 2-cocycles modulo 2-coboundaries is denoted $H^2(C', N)^{sym}$.

We can also formulate all of the above in the category of k-modules: then an extension is Hochschild if it splits in the category k-Mod. In this case the k-module quotient of symmetric 2-cocycles modulo 2-coboundaries is denoted $H^2_k(C', N)^{sym}$.

We can summarize the above discussion as follows.

Lemma 29.3.1. *Given a k-algebra C' and a C'-module N, there is a canonical bijection*

$$\Big\{\textit{Hochschild extns of } C' \textit{ by } N\Big\}/\cong \iff H^2_k(C', N)^{sym}.$$

29.4. **Relation of Hochschild extensions to smoothness.** Assume A is projective over the ring k (e.g. k could be a field). Let N denote an $A -_k A$-bimodule (i.e. a $A \otimes_k A^{op}$-module). In the next subsection we are going to define **Hochschild (co)homology** groups $H^n_k(A, N)$ (resp. $H^k_n(A, N)$) for all $n \geq 0$.

Here is the connection with the notion of smoothness. Consider a diagram

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow{\scriptstyle q} \\ k & \longrightarrow & C, \end{array} \tag{29.4.1}$$

where $N^2 = 0$. This gives rise to a Hochschild extension $E := \{(a, c) \in A \times C \mid v(a) = q(c)\}$ in k-alg. (We used A is projective over k.) We represent the extension as

$$0 \longrightarrow N \xrightarrow{i} E \xrightarrow{\epsilon} A \longrightarrow 0, \tag{29.4.2}$$

where $i(n) = (0, n)$ and $\epsilon(a, c) = a$.

Note that in (29.4.1), v lifts to a k-algebra map $v' : A \to C$ iff the extension E in (29.4.2) is trivial as a k-algebra extension: there exists a k-algebra map $s : A \to E$ such that $\epsilon \circ s = \mathrm{id}_A$.

Therefore,

$$\begin{aligned} A/k \text{ is smooth} &\iff \text{every extension (29.4.2) splits in } k\text{-alg} \\ &\iff H^2_k(A, N)^{sym} = 0 \text{ for every } N \text{ arising from (29.4.1).} \end{aligned}$$

In summary, we have

Proposition 29.4.1. *Let A be a projective k-algebra. Then A/k is smooth iff $H^2_k(A,N)^{sym}=0$ for all A-modules N.*

Proof. Any N as in (29.4.1) is a C/N-module hence (via v) is an A-module. Conversely, given an A-module N, let $C=A*N$, which contains N as an ideal such that $N^2=0$. Thus N appears in a diagram of the form (29.4.1). Now, the proposition follows from our discussion above. □

29.5. **Hochschild (co)homology.** In this subsection k denotes a ring, and A denotes a k-algebra (not necessarily commutative!). Let M denote an $A-_k A$-bimodule, that is, a left $A^e:=A\otimes_k A^{op}$-module. The ring A is itself an A^e-module, via the homomorphism $\varepsilon: A\otimes_k A\to A$ given by $a\otimes b\mapsto ab$.

For $n\geq 0$, we define the **Hochschild cohomology** by

$$H^n_k(A,M):=\mathrm{Ext}^n_{A^e}(A,M),$$

and the **Hochschild homology** by

$$H^k_n(A,M):=\mathrm{Tor}^{A^e}_n(A,M).$$

Recall that if $0\leftarrow A\leftarrow P_0\leftarrow P_1\leftarrow\cdots$ is an A^e-free resolution of A, then

$$\mathrm{Ext}^n_{A^e}(A,M)=H^n(\mathrm{Hom}_{A^e}(P_\bullet,M))$$
$$\mathrm{Tor}^{A^e}_n(A,M)=H_n(P_\bullet\otimes_{A^e}M).$$

This is useful, as we can construct a very simple and explicit resolution $A\leftarrow P_\bullet$ as follows. For simplicity, at this point we assume A is k-free. Let us define

$$\begin{aligned}X_0&=A\otimes_k A=A^e\\ X_1&=A\otimes_k A\otimes_k A\\ &\cdots\\ X_n&=A^{\otimes_k n+2}\cong A^e\otimes_k X_{n-2}.\end{aligned}$$

Note that X_n is an A^e-module by $(a\otimes b)\cdot(x_0\otimes\cdots\otimes x_{n+1})=ax_0\otimes\cdots\otimes x_{n+1}b$. As A^e-modules we have

$$X_n\cong A^e\otimes_k X_{n-2}$$

given by $a\otimes x\otimes b\mapsto(a\otimes b)\otimes x$. Therefore, since X_{n-2} is k-free, we see that X_n is A^e-free, for all n. Thus, we can define an A^e-free resolution $A\leftarrow P_\bullet$ by

$$0\longleftarrow A\xleftarrow{\varepsilon}X_0\xleftarrow{d_1}X_1\xleftarrow{d_2}X_2\xleftarrow{d_3}\cdots$$

where $d_n: X_n=A^{\otimes_k n+2}\to A^{\otimes_k n+1}=X_{n-1}$ is given by

$$d_n(x_0\otimes\cdots\otimes x_{n+1})=\sum_{i=0}^{n}(-1)^i\,x_0\otimes\cdots\otimes x_ix_{i+1}\otimes\cdots\otimes x_{n+1}.$$

It is clear that ε and each d_n is A^e-linear. Moreover, it is easy to see $d_n\circ d_{n+1}=0$ for all $n\geq 0$ (by convention, $d_0=\varepsilon$). Why is the sequence exact? This follows from the existence of "contracting homomorphisms"

$$A\xrightarrow{s_{-1}}X_0\xrightarrow{s_0}X_1\xrightarrow{s_1}\cdots$$

such that

$$\begin{aligned} \varepsilon\, s_{-1} &= \mathrm{id}_A \\ d_1\, s_0 + s_{-1}\, \varepsilon &= \mathrm{id}_{X_0} \\ d_{n+1}\, s_n + s_{n-1}\, d_n &= \mathrm{id}_{X_n}, \end{aligned}$$

the latter holding for all $n \geq 1$. For each $n \geq -1$, set

$$s_n(x_0 \otimes \cdots \otimes x_{n+1}) := 1 \otimes x_0 \otimes \cdots \otimes x_{n+1}.$$

Now we want to use this explicit resolution to identify $H^n_k(A, M)$ more concretely. As stated above, we know that

$$H^n_k(A, M) = H^n\Big[0 \to \mathrm{Hom}_{A^e}(X_0, M) \to \mathrm{Hom}_{A^e}(X_1, M) \to \cdots\Big].$$

Now

$$\begin{aligned} \mathrm{Hom}_{A^e}(X_n, M) &= \mathrm{Hom}_{A^e}(X_{n-2} \otimes_k A^e, M) \\ &= \mathrm{Hom}_k(A^{\otimes_k n}, M) \\ &= C^n(A, M), \end{aligned}$$

where $C^n(A, M)$ denotes the additive group of all k-bilinear maps $A^n \to M$.

Define $\delta : C^n(A, M) \to C^{n+1}(A, M)$ by setting $\delta\, f(x_1, \ldots, x_{n+1})$ to be

$$x_1 f(x_2, \ldots, x_{n+1}) + \sum_{i=1}^{n} (-1)^i\, f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n) x_{n+1}.$$

The commutativity of the diagram (check it!)

$$\begin{array}{ccc} \mathrm{Hom}_{A^e}(X_n, M) & \longrightarrow & \mathrm{Hom}_{A^e}(X_{n+1}, M) \\ \cong \downarrow & & \cong \downarrow \\ C^n(A, M) & \xrightarrow{\ \delta\ } & C^{n+1}(A, M) \end{array}$$

yields

Theorem 29.5.1.

$$H^n_k(A, M) = \frac{\ker(\delta : C^n(A, M) \to C^{n+1}(A, M))}{\mathrm{im}(\delta : C^{n-1}(A, M) \to C^n(A, M))}.$$

Let us see explicitly what elements in $H^2_k(A.M)$ look like with the present definition. A function $f : A \times A \to M$ satisifes $\delta(f(a, b, c) = 0$ iff

$$af(b, c) - f(ab, c) + f(a, bc) - f(a, b)c = 0,$$

that is, iff f is a 2-cocycle in our earlier terminology.

Further, given a function $g : A \to M$, we have

$$\delta g(a, b) = ag(b) - g(ab) + g(a)b.$$

Thus, δg is precisely a 2-coboundary in our earlier terminology. Hence, we conclude that $H^2_k(A, M)$ as defined in this subsection agrees with the definition given in subsection 29.3.

29.6. **Proof of the fundamental fact, Theorem 28.4.1.** We now prove that K/k is smooth $\Leftrightarrow$ is it separable.

Proof.
($\Leftarrow$): We will use Proposition 29.4.1. Hence, we must prove that for a K-module N, we have $H^2_k(K,N)^{sym} = 0$.

We may write $K = \cup_i L_i$, where each L_i/k is a finitely generated and separable (hence separably generated) field extension.

Lemma 29.6.1. *Any separably generated field extension L/k is smooth.*

Proof. Pure transcendental extensions are smooth (why?). Separable algebraic extensions are 0-étale (Lemma 27.2.1), hence smooth. The result now follows by the transitivity property of smoothness. □

Hence by Proposition 29.4.1, we have $H^2_k(L_i,N)^{sym} = 0$ for all i. From this, it follows that $H^2_k(K,N)^{sym} = 0$.

Let's check this last statement in the case where K has countable transcendence degree over k (for the general case, see [Mat1]). In this case, we can write $K = \cup_i L_i$ as a countable directed union. That is, we may assume

$$\cdots \subset L_i \subset L_{i+1} \subset \cdots .$$

Let f be a symmetric 2-cocycle, $f : K \times K \to N$. By hypothesis, $f|_{L_i} = \delta g_i$, where $g_i : L_i \to N$, for each i. We want to "glue" the g_i's to get a function $g : K \to N$ such that $f = \delta g$. The obvious problem is, $g_{i+1}|_{L_i}$ might not be g_i. The idea is to alter g_{i+1} so that this is true (without disturbing the property $\delta g = f$).

Note that $\delta(g_i - g_{i+1}|_{L_i}) = 0$, so that $g_i - g_{i+1}|_{L_i} : L_i \to N$ is a k-derivation. Since L_{i+1}/k is a f.g. separably generated extension, so is L_{i+1}/L_i. (Why? It's enough to check that $L_{i+1} \otimes_{L_i} L'$ is reduced for any field $L' \supset L_i$. But this embeds into $(L_{i+1} \otimes_k L_i) \otimes_{L_i} L' = L_{i+1} \otimes_k L'$, which is reduced since L_{i+1}/k is separable.) Since L_{i+1}/L_i is f.g. separably generated, hence 0-smooth, the splitting of the first fundamental sequence for $k \to L_i \to L_{i+1}$ shows that the natural restriction map

$$\mathrm{Der}_k(L_{i+1}, N) \to \mathrm{Der}_k(L_i, N)$$

is surjective. Thus, we can extend $g_i - g_{i+1}|_{L_i}$ to a k-derivation $\widetilde{g_i - g_{i+1}|_{L_i}} : L_{i+1} \to N$. Now replace g_{i+1} with $g_{i+1} + (g_i - g_{i+1}|_{L_i}) : L_{i+1} \to N$. This new g_{i+1} has

$$f|_{L_{i+1}} = \delta g_{i+1}$$
$$g_{i+1}|_{L_i} = g_i.$$

Continuing in this way, we can "glue" the g_i's together to get $g : K \to N$ such that $f = \delta g$. Thus, $H^2_k(K,N)^{sym} = 0$, as desired. This completes the proof of ($\Leftarrow$).

($\Rightarrow$): Let $k' \supset k$ be a field extension. We need to show that $K \otimes_k k'$ is reduced. It is enough to prove this in the case where k'/k is finite. Why? First, it is clearly enough to consider the case where k'/k is a f.g. field extension. Then let $\Gamma \subset k'$ be a transcendence basis for k'/k and note that

$$K \otimes_k k' = (K \otimes_k k(\Gamma)) \otimes_{k(\Gamma)} k'.$$

Now our reduction to the case "k'/k is finite" follows: $K \otimes_k k(\Gamma)$ is a smooth $k(\Gamma)$-algebra, and the algebraic extension $k'/k(\Gamma)$ is a union of finite algebraic extensions.

Thus, we henceforth assume k'/k is finite. Then $K \otimes_k k'$ is a finite dimensional K-vector space, hence is an Artinian ring. By Atiyah-Macdonald Theorem 8.7,

$$K \otimes_k k' = A_1 \times \cdots \times A_r,$$

where each A_i is an Artinian local ring, and a finite-dimensional K-algebra. Now $K \otimes_k k'$ is smooth over k' implies (exercise) that each A_i is smooth over k'. Therefore by Proposition 28.6.1, each A_i is a regular local ring. But regular local rings are domains, and thus each A_i is actually a field. But then $K \otimes_k k'$ is reduced, as desired. This completes the proof of ($\Rightarrow$). □

29.7. **Geometric regularity, and final remarks.**

Theorem 29.7.1. *Let $(A, \mathfrak{m}, K)$ be a Noetherian local ring, containing a field k. Let $\widehat{A}$ denote the $\mathfrak{m}$-adic completion of A. Suppose K/k is separable. Then TFAE:*

1. *A is regular.*
2. *$\widehat{A} \cong K[[X_1, \ldots, X_d]]$ as K-algebras and as k-algebras too (where $d = \dim(A)$).*
3. *$\widehat{A}$ is fs over k.*
4. *A is fs over k.*

Proof. (1) $\Rightarrow$ (2): Since $\widehat{A}$ is complete and regular, and contains k, (2) follows from the Cohen Stucture theorem (Corollary 28.2.2).
(2) $\Rightarrow$ (3): Clear since then $\widehat{A}$ fs over K and K fs over k (since K/k separable; use Theorem 28.4.1).
(3) $\Leftrightarrow$ (4): Lemma 28.2.4.
(4) $\Rightarrow$ (1): Proposition 28.6.1. □

For now on, assume $(A, \mathfrak{m})$ is a Noetherian local ring, and contains a field k.

Lemma 29.7.2. *If B is a finite A-module, then B is semi-local.*

Proof. Note that $B/\mathfrak{m}B$ is a finite $A/\mathfrak{m}$-module, hence is Artin, and thus has finitely many maximal ideals. The maximal ideals of B all lie over $\mathfrak{m}$ (by the Going-Up theorem), so B has only finitely many maximal ideals. Thus B is semi-local. □

In particular, for every finite extension $k' \supset k$, the ring $A' := A \otimes_k k'$ is semi-local. Recall that we say such a ring is **regular** provided all of its localizations at maximal ideals are regular. We say A is **geometrically regular** over k if $A' := A \otimes_k k'$ is regular, for every finite extension k'/k.

Lemma 29.7.3. *If $A/\mathfrak{m}$ is separable over k, then*

$$\begin{aligned} A \text{ is regular} &\Longleftrightarrow A \text{ is fs over } k \\ &\Longrightarrow A' \text{ is fs over } k' \\ &\Longrightarrow A' \text{ is regular.} \end{aligned}$$

Proof. Only the final implication needs explanation. It does not follow immediately from Proposition 28.6.1 because A' is not local, but only semi-local. Nevertheless, if $\mathfrak{n} \subset A'$ is a maximal ideal, then $A'_{\mathfrak{n}}$ is fs over k' (recall $A'_{\mathfrak{n}}/A'$ is 0-étale), and then Proposition 28.6.1 yields $A'_{\mathfrak{n}}$ is regular for each $\mathfrak{n}$. Thus A' is regular. □

Thus, in case $A/\mathfrak{m}$ is separable over k, we have "regular" $\Leftrightarrow$ "geometrically regular". In general, we can say the following.

Proposition 29.7.4. *Suppose $(A, \mathfrak{m}, K)$ be Noetherian local, containing a field k. Then A is fs over k iff A is geometrically regular over k.*

Proof. ($\Rightarrow$): If A is fs over k, then A' is fs over k', and then the proof of the Lemma above shows that A' is regular. Thus A is geometrically regular over k.
($\Leftarrow$): (Sketch; we consider only the case where K/k is a f.g. field extension.) Take a radiciel extension $k' \supset k$ such that $K(k')$ is separable over k'. Then $A' := A \otimes_k k'$ is regular, and has residue field $K(k')$. So A' is fs over k'. We conclude that A is fs over k by invoking the following lemma. □

Lemma 29.7.5. *Let A be a topological ring containing a field k. Let $k' \supset k$ be a k-algebra endowed with the discrete topology. Then A is fs over k iff $A' := A \otimes_k k'$ is fs over k'.*

Proof. We assume A' is fs over k'; we need to prove A is fs over k. Consider the usual diagram

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow \\ k & \longrightarrow & C. \end{array}$$

Tensoring the diagram with $- \otimes_k k'$ yields a diagram

$$\begin{array}{ccc} A' & \xrightarrow{v'} & C'/N' \\ \uparrow & \overset{w}{\searrow} & \uparrow \\ k' & \longrightarrow & C' \end{array}$$

where $C' = C \otimes_k k'$, $N' = N \otimes_k k'$, and $v' = v \otimes_k \mathrm{id}_{k'}$. The lifting w exists since A'/k' is fs.

Now choose a k-submodule V of k' such that $k' = k \oplus V$ as k-vector spaces. Note that $C' = C \oplus (C \otimes V)$, and $C \otimes V$ is a C-submodule of C'. Write

$$w(a) = u(a) + r(a),$$

where $u(a) \in C$ and $r(a) \in C \otimes V$, for $a \in A$. Since the image of $w(a)$ modulo N' is $v(a) \in C/N$, we see that $r(a) \in N \otimes V$, for all $a \in A$. This implies that $r(a)r(b) = 0$, for $a, b \in A$. Thus $u : A \to C$ is a k-algebra homomorphism, lifting v. This shows that A is fs over k, as desired. □

References

[Mat1] H. Matsumura, *Commutative Algebra*.
[Mat2] H. Matsumura, *Commutative Ring Theory*, Camb. stud. in adv. Math. **8**, Cambridge Univ. Press, 1992, 320 pp. + xiii.
[Serre] J.-P. Serre, *Local Algebra*, Springer Monographs in Math., 2000.