# A course in
# Commutative Algebra

Taught by N. Shepherd-Barron

Michaelmas 2012

*Last updated: May 31, 2013*

## Disclaimer

These are my notes from Nick Shepherd-Barron's Part III course on commutative algebra, given at Cambridge University in Michaelmas term, 2012. I have made them public in the hope that they might be useful to others, but these are not official notes in any way. In particular, mistakes are my fault; if you find any, please report them to:

Eva Belmont
ekbelmont@gmail.com

Contents

# Lecture 1: October 5

## Chapter 1: Noetherian rings

Definition 1.1. Rings are commutative with unit, homomorphisms take $1 \mapsto 1$, and modules are unital ($1 \cdot m = m$). If $R$ is a ring, then an $R$-algebra is a ring $A$ with a specified homomorphism $R \to A$. An ideal $I$ of a ring $A$ is *prime* if $I \neq A$ and $A/I$ is a domain. Equivalently (do this!), whenever $xy \in I$, then either $x \in I$ or $y \in I$. An ideal is maximal if $I \neq A$, and every ideal $J$ with $I \subset J \subset A$ is either $J = I$ or $J = A$. Equivalently, $A/I$ is a field.

Lemma 1.2. *Suppose $M$ is an $A$-module. Then TFAE:*

(1) *Every ascending chain $\cdots \subset M_n \subset M_{n+1} \subset \cdots$ of submodules of $M$ stabilizes: there exists $n_0$ such that $M_{n_0} = M_{n_0+1} = \cdots$.*
(2) *Every submodule $N$ of $M$ is finitely generated: there exist $n_1, \cdots, n_r \in N$ such that every element can be written $\sum a_j n_j$ with $a_j \in A$.*
(3) *Every nonempty set of submodules of $M$ has a maximal element.*

*Proof.* Exercise. ○

Definition 1.3. $M$ is Noetherian if it satisfies any of the preceding conditions. The ring $A$ is Noetherian if it is Noetherian as a module over itself. (In this case the submodules of the ring are precisely the ideals.) So, a ring is Noetherian iff every ideal is finitely generated.

Rings of differentiable functions are not Noetherian. Commutative algebra is not adequate as a foundation for the geometry of manifolds – you need calculus.

If $B$ is an $A$-algebra, then $B$ is finitely generated ("of finite type in $A$") if $B \cong A[X_1, \cdots, X_n]/I$. If $B$ is an $A$-algebra, and is finitely-generated as an $A$-module, then we say that $B$ is finite over $A$. (Being finitely generated as a module is much stronger than being finitely generated as an algebra.)

Exercise 1.4. If $A$ is a Noetherian ring, and $M$ is a finitely-generated $A$-module, then $M$ is Noetherian. (Hint: use induction on the number of generators of $M$.)

Theorem 1.5 (Hilbert Basis Theorem). *If $A$ is Noetherian, then $A[X]$ is also Noetherian.*

*Proof.* Suppose $I$ is an ideal. Define $J$ to be the subset of $A$ consisting of the leading coefficients of the elements of $I$, and add in 0. Now check that $J$ is an ideal in $A$. Every ideal has a finite generating set, so say $J = (j_1, \cdots, j_n)$. Choose $f_i \in I$ with leading coefficient $j_i$. Let $N = \max\{\deg f_i\}$. Let $M = \{f \in A[X] : \deg f \leq N\}$. $M$ is generated by $\{1, X, \cdots, X^N\}$ as an $A$-module. Now $M \cap I$ is a sub-$A$ module of $M$. Using the above exercise, $M \cap I$ is finitely generated; say $g_1, \cdots, g_m$ are generators. So each $g_i \in I$, and it has degree at most $N$.

***Claim:*** *The $f_i$'s and the $g_j$'s together generate $I$.*

Let $h \in I$, and $\deg h = d$. If $d \leq N$, then $h \in I \cap M$, and so it is a linear combination of the $g_i$'s. If $d \geq N+1$, let $b$ denote the leading coefficient of $h$. Then $b \in J$, so I can write $b$ as an $A$-linear combination of the $j_i$'s. Recall that the $f_i$'s have leading coefficients $j_i$. Say $\deg f_i = e_i \leq N$. Then $h_1 = h - \sum a_i f_i X^{d-e_i} \in I$ because $h \in I$ and each $f_i \in I$, and it has degree $< \deg h$: we cooked up this expression to annihilate $b$. By induction on the degree, $h_1$ is a linear combination of the $g_i$'s and $f_i$'s, and therefore $h$ is as well. ○

Corollary 1.6. *If $A$ is Noetherian, then every $A$-algebra of finite type is also Noetherian.*

Example 1.7.

- $\mathbb{Z}$ is Noetherian because it is a PID: every ideal is generated by one element, and 1 is finite.
- Every field is Noetherian, because there aren't any (nontrivial) ideals.
- Every affine algebraic variety (it's finitely generated over a field) is Noetherian.

---

## Chapter 2: Localization

Definition 1.8. A subset $S$ of a ring $A$ is multiplicative if $1 \in S$, $0 \notin S$, and $S$ is closed under multiplication.

For example, $\mathbb{Z} - \{0\}$ is a multiplicative set.

Definition 1.9. For multiplicative $S$, define $S^{-1}A = S \times A/\sim$, where $(s,a) \sim (s',a')$ if there exists $s'' \in S$ such that $s''(as' - a's) = 0$. (If $A$ is an integral domain, you don't need $s''$.) Check that this is an equivalence relation. Write the equivalence class $[(s,a)]$ as $\frac{a}{s}$ or $s^{-1}a$. $S^{-1}A$ is a ring, with addition and multiplication defined with the usual rules of fraction addition and multiplication. The unit is $\frac{1}{1}$, and $\frac{0}{1}$ is the zero element. Moreover, it is an $A$-algebra, via the map $a \mapsto \frac{a}{1}$.

Suppose $A$ is a domain. Then $S = A - \{0\}$ is a multiplicative set, and $S^{-1}A = Frac(A)$. For any $S$, we have $A \subset S^{-1}A \subset Frac(A)$. If $M$ is an $A$-module, we can construct an $S^{-1}A$-module $S^{-1}M$ in a similar way.

Example 1.10.

- $\mathfrak{P}$ is a prime ideal and $S = A - P$. Write $S^{-1}A = A_{\mathfrak{P}}$.
- Let $s \in A$, where $s$ is not nilpotent. Then take $S = \{s^n : n \in \mathbb{N}\}$. This gives
$$S^{-1}A = A[S^{-1}] \cong A[X]/(Xs - 1)$$
.

# Lecture 2: October 8

**Localization.** Every ideal $J$ of $S^{-1}A$ can be written as $J = S^{-1}I$, where $I$ is some ideal in $A$ (not necessarily a unique choice). This shows that every $J$ is Noetherian if $A$ is Noetherian.

PROPOSITION 2.1. *(2.3) There is an inclusion-preserving bijection*

$$\{\textit{prime ideals of } A \textit{ disjoint from } S\} \iff \{\textit{prime ideals of } S^{-1}A\}$$

*where* $Q \mapsto S^{-1}Q$.

*Proof.* Exercise. *$I \subset A$ prime. If $\frac{a}{s} \cdot \frac{b}{t} = \frac{i}{\sigma}$ then $\sigma \cdot a \cdot b = i \cdot s \cdot t \in I$ and $\sigma \notin I$ so $a$ or $b$ is in $I$. Conversely, if $\varphi : A \to S^{-1}A$ is the obvious map then $\varphi^{-1}(J)$ is prime if $J \subset S^{-1}A$ is prime.* ○

If $S = A - P$, then the prime ideals in $A_P$ correspond exactly to the prime ideals of $A$ that are contained in $P$. Also, prime ideals of $A/I$ correspond to prime ideals of $A$ that contain $I$.

DEFINITION 2.2. (2.4) A *quasi-local ring* is a ring with a unique maximal ideal. A *local ring* is a Noetherian quasi-local ring.

For example, $A_P$ is a quasi-local ring, whose unique maximal ideal is $P_P = S^{-1}P$.

DEFINITION 2.3. (2.5) The *nilradical* $\mathrm{nil}(A)$ is the set of nilpotent elements of $A$.

PROPOSITION 2.4. *(2.6)*

$$\mathrm{nil}(A) = \bigcap(\textit{prime ideals of } A)$$

The proof is easier if you assume the ring is Noetherian; otherwise you need the Axiom of Choice.

*Proof.* Clearly $\mathrm{nil}(A) \subset P$ for all primes $P$ *because if $n^i = 0$ then $n \cdot n^{i-1} = 0 \in P$ since zero is in every ideal, $\implies$ $n \in P$ or $n^{i-1} \in P$; continue by induction.* Conversely, suppose $s \in A$ is not nilpotent. Then set $S = \{s^n\}$. Then $S^{-1}A$ is a nonzero ring. We need the following lemma.

LEMMA 2.5. *(2.7) Every nonzero ring has a maximal ideal.*

*Proof of Lemma 2.7. We will use Zorn's lemma on the set of proper ideals. Any totally ordered chain $\cdots \subset I_\alpha \subset \cdots$ has an upper bound $\bigcup I_\alpha$, which is also proper. So Zorn's lemma gives a maximal element in the set of proper ideals.* ○

So $S^{-1}A$ has a maximal ideal, so a prime ideal, say $S^{-1}P$. By Proposition 2.3, $s \notin P$. *Let $\mathfrak{m} \subset S^{-1}A$ be a maximal ideal; in particular, it is prime. Then $s \notin \mathfrak{m}$ by design (else $\mathfrak{m}$ would be the whole ring $S^{-1}A$), which means $s \notin \mathfrak{m} \cap A$, and $\mathfrak{m} \cap A$ is a prime ideal of $A$ (the inverse image along the inclusion... I'm assuming it's an inclusion, similar otherwise.) So $s \notin \mathrm{nil}(A) \implies s \notin \bigcap_{primes} \mathfrak{P}$.* ○

COROLLARY 2.6. *If $I \subset A$ is an ideal then*

$$\sqrt{I} = \bigcap(\textit{prime ideals } \supset I)$$

*Proof.* Use the previous lemma with $A/I$ as the ring...

$$\bigcap(\text{primes of } A/I) \iff \bigcap(\text{primes of } A \text{ containing } I)$$

○

DEFINITION 2.7. The Jacobson radical of $A$, $\mathrm{rad}(A)$ is the intersection of all maximal ideals of $A$.

(So in a local ring, the Jacobson radical is the unique maximal ideal.)

## CHAPTER 3: INTEGRAL EXTENSIONS

PROPOSITION 2.8 (Cayley-Hamilton). *(3.1) Let $A$ be a ring, $I$ an ideal, $M$ a finitely-generated $A$-module, $\varphi : M \to M$ an $A$-endomorphism such that $\varphi(M) \subset I \cdot M$. Then, there exist $a_i \in I$ such that*

$$\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 = 0$$

*is an identity of endomorphisms of $M$.*

*Proof.* Pick generators $x_1, \cdots, x_n$ of $M$. Say $\varphi(x_i) = \sum a_{ij}x_j$ where $a_{ij} \in I$ (restating hypothesis that $\varphi(M) \subset I \cdot M$).

Note $A[\varphi] \subset End_A(M)$ is a commutative subring of the noncommutative ring $End_A(M)$ (endomorphisms are not commutative because matrix multiplication is noncommutative). Furthermore, $M$ is an $A[\varphi]$-module. From above,

$$\sum_j (\delta_{ij}\varphi - a_{ij})x_j = 0 \tag{2.1}$$

for all $i$. Think of $(\delta_{ij}\varphi - a_{ij})$ as an $n \times n$ matrix $N$ with entries in $A[\varphi]$:

$$\begin{pmatrix} \varphi - a_{11} & -a_{12} & -a_{13} \\ \cdots & \varphi - a_{22} & \\ & & \varphi - a_{33} \end{pmatrix}$$

So $N : M^{\oplus n} \to M^{\oplus n}$, where $M^{\oplus n}$ contains column vectors with entries in $M$.

Then (2.1) says that $N \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0$. Let $N'$ be the adjugate of $N$ (the transposed matrix of cofactors). So $N'N = (\det N)\mathbb{1}_n$.

So $(\det N)x_j = 0$ for all $j$, which implies that $\det N = 0$ in $End_A(M)$. In order to get the identity in the proposition, just expand the determinant of the matrix we're constructed.

○

COROLLARY 2.9 (Nakayama's Lemma). *(3.2) Suppose $I \subset \mathrm{rad}(A)$, $M$ is a finite*[1] *$A$-module and $I \cdot M = M$. Then $M = 0$.*

*Proof.* Take $\varphi = 1$ in Cayley-Hamilton. Then we get

$$1 + a_{n-1} + \cdots + a_0 = z$$

where $z$ is the zero endomorphism (so $z \cdot M = 0$). But the $a_i \in \mathrm{rad}(A)$, and are each in all maximal ideals. $z = 1 + \cdots$ lies in no maximal ideal, and is a unit. Since $z \cdot M = 0$ for a unit $z$, we have $M = 0$. ○

*The following corollary, copied from Eisenbud p.124, will be useful later:*

COROLLARY 2.10. *Suppose $I \subset \mathrm{rad}\, A$ and $M$ is a finitely generated $A$-module. If $m_1, \cdots, m_n \in M$ have images in $M/IM$ that generate it as an $A$-module, then $m_1, \cdots, m_n$ generate $M$ as an $A$-module.*

*Proof.* Apply Nakayama's Lemma to the module $N = M/\langle m_1, \cdots, m_n \rangle$. (To show the condition $N = I \cdot N$ is fulfilled, check that $I + \langle m_1, \cdots, m_n \rangle$ generates $M$, so $N/IN = 0$ as desired.) ○

Fix a ring $A$, an $A$-algebra $B$, and a morphism $A \to B$. For simplicity assume $A \subset B$.

DEFINITION 2.11. $z \in B$ is *integral over $A$* if it satisfies a monic polynomial in $A[T]$.

PROPOSITION 2.12. *(3.4) TFAE:*

(1) *$z$ is integral over $A$*
(2) *$A[z] \subset B$ is a finite $A$-module*
(3) *$z$ lies in a subring $C$ of $B$, with $A \subset C \subset B$, and $C$ a finite $A$-module*
(4) *There exists a faithful $A[z]$-module $M$ that is finite as an $A$-module*

*Proof.* (1) $\implies$ (2). Suppose I have a monic relation $\sum_0^n a_i z^i = 0$ with $a_n = 1$. Then $\{1, z, \cdots, z^{n-1}\}$ generate $A[z]$ as an $A$-module (since you can write $z^n = -\sum_0^{n-1} a_i z^i$).

(2) $\implies$ (3). Take $C = A[z]$.

(3) $\implies$ (4). Take $M = C$.

(4) $\implies$ (1). Use Cayley-Hamilton. Take $\varphi$ to be multiplication by $z$, $I = A$. Then $z^n + a_{n-1} z^{n-1} + \cdots + a_0 = 0$ for $a_i$, as an endomorphism of $M$. But faithfulness says that anything that kills the entire module must be zero in the ring. So $z^n + \cdots + a_0 = 0$ in $A[z]$; this is (1). ○

The point is to say something about the prime ideals in $B$ as they relate to the prime ideals of $A$, if $B$ is finite over $A$.

[1] for modules, finite := finitely-generated

COROLLARY 2.13. *(3.5) Suppose $x_1, \cdots, x_n \in B$ are each integral over $A$. Then $A[x_1, \cdots, x_n]$ is a finite $A$-module.*

*Proof.* Induction on $n$, and Proposition 3.4. ○

COROLLARY 2.14. *(3.6) If*

$$C = \{x \in B : x \text{ is integral over } A\}$$

*then $C$ is a ring.*

*Proof.* If $x, y \in C$, then $A[x, y]$ is finite over $A$ by Corollary 3.5. But $x \pm y, xy \in A[x, y]$, and $A[x, y]$ is faithful as a module over each ring $A[x+y], A[x-y], A[xy]$ *(because $A[x+y] \subset A[x, y]$, and any annihilator of $A[x, y]$ would also have to kill all of $A[x+y]$, esp. 1)*. Now use (4) $\implies$ (1) in Proposition 3.4. ○

DEFINITION 2.15. $B$ is integral over $A$ if every element of $B$ is integral over $A$.

COROLLARY 2.16 (Transitivity of integral dependence). *(3.8) Suppose $A \subset B \subset D$. If $B$ is integral over $A$, and $D$ is integral over $B$, then $D$ is integral over $A$.*

*Proof.* Let $x \in D$. Then $\sum_0^n b_i x^i = 0$ for $b_i \in B$, $b_n = 1$. Then $B' = A[b_0 \cdots b_{n-1}]$ is a finite $A$-module, and $B'[x]$ is a finite $B'$-module. So $B'[x]$ is finite over $A$. Now $B'[x]$ is a faithful $A[x]$-module, since $A[x] \subset B'[x]$. Now apply Proposition 3.4 again. ○

# LECTURE 3: OCTOBER 10

**More integral extensions.**

LEMMA 3.1. *Suppose $A \subset B$, $B$ is integral over $A$.*

(1) *If $J$ is an ideal in $B$, and $I = J \cap A$ then $B/J$ is integral over $A/I$.*
(2) *If $S \subset A$ is multiplicative then $S^{-1}B$ is integral over $S^{-1}A$.*

*Proof.* Exercise. ○

LEMMA 3.2. *(3.11) If $A \subset B$ are domains, with $B$ integral over $A$ then $A$ is a field iff $B$ is a field.*

(The idea is that, in an integral extension of rings, the primes of one ring are related to the primes of the other.)

*Proof.* Exercise. ○

DEFINITION 3.3. A domain $A$ is *normal* if it is integrally closed in the field of fractions.

THEOREM 3.4. *(3.13) Suppose $A$ is a normal Noetherian domain, $Frac(A) = K$, and $L$ is a finite separable extension of $K$. Let $B$ be the integral closure of $A$ in $L$. Then $B$ is a finite $A$-module.*

*Proof.* Enlarging $L$ is harmless, so we may assume that $L/K$ is Galois, with Galois group $G = \{s_1, \cdots, s_n\}$. For all $x \in L$, $tr(x) = tr_{L/K}(x)$ is the trace of $x$ as a $K$-linear map $L \xrightarrow{x} L$. The trace is also the constant term of the characteristic polynomial (and therefore the sum of the roots), so $tr(x) = \sum s_i(x)$. Recall that a finite extension of fields $L/K$ is separable iff the bilinear mapping

$$T = (-,-) : L \times L \to K \text{ where } (x,y) = tr(xy)$$

is nondegenerate. (Proof in characteristic 0: suppose $x \neq 0, x \in L$ such that $(x,y) = 0$ for all $y \in L$. Then take $y = x^{-1}$, to get $tr(xy) = tr(1) = 0$. But $tr(1) = [L : K] \neq 0$ (by characteristic zero-ness).)

Pick a $K$-linear basis $(y_1, \cdots, y_n)$ of $L$, contained in $B$. Note that $s_i(y_j) \in B$. Let $M$ be the matrix with entries $s_i(y_j)$. Then ${}^tMM = (tr(y_i y_j))$. The trace is nondegenerate, and therefore $\det M \neq 0$. Now suppose $z \in B$. Write $z = \sum c_j y_j$ with $c_j \in K$. So

$$s_i(z) = \sum_j c_j \cdot s_i(y_j). \tag{3.1}$$

Note that $s_i(z) \in B$ as before. Let $d = \det(tr(y_i y_j))$ and $D = \det M$; then $D^2 = d$ and $d \in K$. We can rewrite (3.1) in matrix form:

$$\begin{bmatrix} s_1(y_1) & s_1(y_2) & \cdots \\ & \ddots & \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} s_1(z) \\ \vdots \\ s_n(z) \end{bmatrix}$$

or equivalently

$$\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = M^{-1} \cdot \begin{bmatrix} s_1(z) \\ \vdots \\ s_n(z) \end{bmatrix} = \frac{1}{\det M} \cdot (C_M)^t \cdot \begin{bmatrix} s_1(z) \\ \vdots \\ s_n(z) \end{bmatrix}$$

where $C_M$ is the matrix of cofactors. Each entry in $C_M$ is a polynomial in entries of $M$, so the entries of $C_M$ are in $B$, and hence $c_j \in D^{-1} \cdot B$. Since $D^2 = d$, we have $d \cdot c_j \in D \cdot B \subset B$. Also $d \cdot c_j \in K$ (we said above $d \in K$, and $c_j \in K$ by definition). Since $A$ is normal, $B \cap K = A$, so $d \cdot c_j \in A$.

So, we showed $z = \sum c_j y_j \in \sum_j (d^{-1}A) \cdot y_j$ for some arbitrary $z \in B$, so in general $B \subset \sum_j A \cdot (d^{-1} y_j)$. Since $A$ is Noetherian, $B$ is of finite type over $A$. *I think we're applying Lemma 1.2, part (2), to an extension of $A$.* ○

COROLLARY 3.5. *(3.14) The integers in an algebraic number field (finite extension of $\mathbb{Q}$) form a ring $\mathcal{O}_K$ which is a finitely-generated $\mathbb{Z}$-module.*

LEMMA 3.6. *(3.15) Suppose $A \subset B$, with $B$ integral over $A$, and $Q$ prime in $B$. Then $Q$ is maximal in $B$ iff $Q \cap A$ is maximal in $A$.*

*Proof.* Immediate corollary of Lemma 3.11. ○

THEOREM 3.7 (Going-up theorem). *(3.16) Suppose $A \subset B$ as above, $P_1 \subset \cdots \subset P_m$ are prime ideals in $A$, $Q_1 \subset \cdots \subset Q_n$ with $n < m$, and such that $Q_i \cap A = P_i$. Then we can extend the chain of $Q_i$'s with new primes, so $Q_n \subset Q_{n+1} \subset \cdots \subset Q_m$ and $Q_i \cap A = P_i$ for all the new $Q_i$'s too.*

*Proof.* Induction reduces to $n = 2$, $m = 1$. Put $S = A - P_2$. Then $S^{-1}(B/Q_1)$ is integral over $S^{-1}(A/P_1)$, which is a quasi-local domain, with unique maximal ideal $P_2/P_1$. Pick any maximal ideal of $S^{-1}(B/Q_1)$. This is $S^{-1}(Q_2/Q_1)$ for some prime ideal $Q_2$, and $Q_2$ does the job. ○

When you mod out by an ideal, you keep just the ideals that contain that ideal. Localizing at a prime does the opposite: you keep only the ones that are disjoint from the original prime.

## CHAPTER 4: NOETHER NORMALIZATION AND THE NULLSTELLENSATZ

Every finitely generated $k$-module is a finite extension of a polynomial ring.

THEOREM 3.8 (Noether normalization lemma). *(4.1) Suppose that $k$ is a field, $A$ a finitely-generated $k$-algebra. Then there is a finitely-generated $k$-algebra $R$ of $A$ such that*

(1) *$R$ is a polynomial ring*
(2) *$A$ is finite over $R$*

*Proof.* Suppose that $A = k[x_1, \cdots, x_r]$ (with $x_i$'s not necessarily independent, just generators). Use induction on $r$. Either $x_1$ does not satisfy any relationship, in which case $A[x_1]$ is a polynomial ring, or $x_1$ satisfies a nontrivial relation, in which case it is integral over $k$ (monic because $k$ is a field and you can just divide out by the leading coefficient).

Now assume $r \geq 2$ and the result holds for all $k$-algebras generated by at most $r - 1$ elements. We can suppose that there is some relation

$$\sum a_n x_1^{n(1)} \cdots x_r^{n(r)} = 0$$

for $a_n \in k$, $a_n \neq 0$ for $n = (n(1), \cdots, n(r)) \neq (0, \cdots, 0)$. Choose $g \in \mathbb{N}$, $g >$ every $n(j)$. For $i \geq 2$, put $z_i = x_i - x_1^{g^{i-1}}$. Then

$$\sum a_n x^{n(1)} (z_2 + x_1^g)^{n(2)} (z_3 + x_1^{g^2})^{n(3)} \cdots = 0$$

In each of these summands, the term of highest degree in $x_1$ is $a_n x_1^{n(1)+n(2)g+n(3)g^2+\cdots+n(r)g^{r-1}}$. These exponents are all different, given they have different expansions to base $g$ (or, "g-adically") (using the fact that $g$ is big). *So the highest-degree terms don't cancel, and the highest-degree term of the whole sum is one of these $a_N x_1^{stuff}$'s. After dividing by this $a_N \in k$,* $x_1$ satisfies a monic relation over $k[z_2, \cdots, z_r] = B$. Then $A = k[x_1, z_2, \cdots, z_r]$. Apply the induction hypothesis to the ring $B$. ○

COROLLARY 3.9 (Weak Nullstellensatz). *(4.2)*

(1) *If $M$ is a maximal ideal in a polynomial ring $A = k[x_1, \cdots, x_n]$, then $A/M$ is finite over $k$. Not sure why $A$ has to be a polynomial algebra, as opposed to just a finitely-generated algebra over $k$.*
(2) *If $k$ is algebraically closed, then there are $a_1, \cdots, a_n \in k$ such that $M$ is generated by $x_1 - a_1, \cdots, x_n - a_n$.*
(3) *If $K/k$ is a field extension with $K$ finitely-generated as a $k$-algebra, then $K$ is finite over $k$.*

*Proof.* (1) By NNL, $A/M$ is finite over a polynomial subring $R$; by Lemma 3.11, $R$ is a field. So $R = k$. *Recall that f.g. as a module $\implies$ integral, by Proposition 3.4.*

(2) If $k = \overline{k}$ then $A/M$ is finite over $k$, and so it must be equal to $k$. (No nontrivial finite extensions of an algebraically closed field.)

(3) If $K = k[x_1, \cdots, x_n]$ then $K = A/M$ with $A = k[x_1, \cdots, x_n]$ and $M$ maximal, (1) says $A$ is finite over $k$. ○

Part (2) says that maximal ideals are all just points *(i.e. points in a variety)*.

# Lecture 4: October 12

**Consequences of the Noether normalization lemma.**

Corollary 4.1 (Strong Nullstellensatz). *Suppose $A = k[X_1, \cdots, X_n]$, and $I$ is an ideal of $A$. Then*

(1) $\sqrt{I} = \bigcap_{M \supset I} M$
(2) *Suppose $k = \overline{k}$. Define $V(I) = \{(a_1, \cdots, a_n) \in k^n : f(a_1, \cdots, a_n) = 0 \ \forall f \in I\}$. ("V" is for "variety".) Suppose $g(a_1, \cdots, a_n) = 0$ for every $(a_1, \cdots, a_n) \in V(I)$. Then $g \in \sqrt{I}$.*

*Proof.* *By Proposition 2.6*, we just need to show that $P = \bigcap_{M \supset P} M$, for all primes $P$. *But actually, we just need to prove that $\bigcap_{M \supset P} M \subset P$, because the other direction is obvious.* Suppose $f \in \bigcap_{M \supset P} M$. Set $\overline{f} = f \pmod{P}$. We need to prove that $\overline{f} = 0$.

Set $R = A/P$. Then by the Noether normalization lemma, $R$ is finite over a polynomial subring $S$. Suppose that $c$ is the constant term of the minimal polynomial of $\overline{f}$ over $S$. Since $R$ is a domain, $c \neq 0$. *If $c = 0$ then you could divide the minimal polynomial by $\overline{f}$ and get a minimal-er polynomial.* We know *(do we? this is apparently because $S \subset R$ is integral... right, use the lemma about integral extensions over a field!)* that every maximal ideal $N$ in $S$ extends to a maximal ideal $N/P$ of $R$. *We designed $\overline{f}$ so that it is in every maximal ideal of $R$; writing the minimal polynomial as $c = -\overline{f}(\text{stuff})$, we see that $c$ is also in every maximal ideal of $R$.* Hence $c \in \bigcap$(max. ideals of $S$).

Exercise: show that this intersection is 0. (e.g. if $k$ is infinite, consider the maximal ideals $(y_1 - a_1, \cdots, y_r - a_r)$ for all $a_1, \cdots, a_r \in k$. Then $c$ is a polynomial function vanishing at every point, so is obviously $= 0$.)

(2) follows from (1) and the weak Nullstellensatz (maximal ideals exactly come from the points in $k^n$, if $k = \overline{k}$). So, if $k = \overline{k}$, then subsets of $\mathbb{A}^n_k$ defined by polynomials correspond exactly to radical ideals in the polynomial ring. ○

THEOREM 4.2. *Suppose $A$ is a finitely-generated $\mathbb{Z}$-algebra. Then for every maximal ideal $M$ of $A$, $A/M$ is a finite field.*

*Proof.* $M \cap \mathbb{Z}$ is certainly a prime ideal in $\mathbb{Z}$, so it's either $(p)$ or 0. If $M \cap \mathbb{Z} = (p)$, then by the weak Nullstellensatz with $k = \mathbb{Z}/p$ we get that $A/M$ is finite over $\mathbb{Z}/(p)$, so finite. (Any ring that is finite over a finite ring is also finite.)

So suppose $M \cap \mathbb{Z} = (0)$. $A/M = \mathbb{Z}[x_1, \cdots, x_n] \supset \mathbb{Z}$. $A/M$ is a field, so $A/M \supset \mathbb{Q}$. The Nullstellensatz again says that $A/M$ is finite over $\mathbb{Q}$. So there exist exponents $b_i x_i^{n_i} + (\text{lower terms}) = 0$, with coefficients in $\mathbb{Z}$. So each $x_i$ is integral over the subring $B = \mathbb{Z}[b_1^{-1}, \cdots, b_n^{-1}] \subset \mathbb{Q}$, and $A/M$ is integral over $B$. The field $A/M$ is integral over the subring $B$, so $B$ is a field, and $B = \mathbb{Q}$. This is obvious nonsense, since there are infinitely many primes. ○

DEFINITION 4.3. A group $G$ is *residually finite* if for all $\mathbb{1} \neq g \in G$, there is a finite group $H$ and a homomorphism $\pi : G \to H$ such that $\pi(g) \neq \mathbb{1}$. (a.k.a. for all $g$ there is a map to a finite group that doesn't kill $g$)

Note that $GL_n(\mathbb{C})$ is not residually finite because it is connected. (Finite groups are the most disconnected things...)

COROLLARY 4.4. *Every finitely generated subgroup $G$ of $GL_n(\mathbb{C})$ is residually finite.*

*Proof.* Take $A$ to be the $\mathbb{Z}$-algebra generated by all matrix entries of some finite generating set of the group, and all the inverses of their determinants. So now $G \subset GL_n(A)$. Let $g = (a_{ij}) \in G$, with $a_{ij} \in A$. Say $a_{11} \neq 1$. Then there is a maximal ideal $M$ of $A$ such that $a_{11} - 1 \notin M$. Then

$$GL_n(A) \xrightarrow{\pi} GL_n(A/M)$$

is a group homomorphism, and $g \not\mapsto 1$. ○

THEOREM 4.5. *Assume that $k$ is a field, and that if $char(k) = p > 0$, then $[k : k^p] < \infty$ (e.g. the field of functions of a variety). Assume that $A$ is a domain, finitely generated over $k$, and $L$ a field such that $L/K$ is finite for $K = Frac(A)$. Let $B$ be the integral closure of $A$ in $L$.*

*Then $B$ is finite over $A$.*

(Earlier result assumed $A$ was integrally closed over its field of fractions, and we had a finite separable extension. Here, you have to assume that $A$ is a domain, f.g. over $k$, but not assuming the other conditions. This could be false for *general* Noetherian domains.) In particular, if $L = K$ then the integral closure of $A$ in Frac$(A)$ is finite over $A$.

*Proof.* By the NNL, $A$ is finite over a polynomial subring $R$. Then $B$ is the integral closure of $R$ in $L$.

Let $L_1$ be the separable closure of $Frac(R)$ in $L$, and $R_1$ the integral closure of $R$ in $L_1$. $R$ is a polynomial domain, hence UFD, hence normal. So $R_1$ is finite over $R$ by Theorem 3.13. $B$ is the integral closure of $R_1$ in $L$, so we can replace $A$ by $R_1$ and $K$ by $L_1$. So we can assume that $A$ is normal, and that $L/K$ is purely inseparable. Because $[k : k^p] < \infty$, there exists some $n$ such that $K_n := K^{(p^{-n})} = \{\alpha : \alpha^{(p^n)} \in K\}$ is finite over $K$, and $K_n \supset L$. *Note that $L$ inseparable means that, if $\alpha \in L$, then $\alpha^{p^n} \in K$ for some $n$.*

$A = k[x_1, \cdots, x_r]$ (finitely generated, not a polynomial ring).

$$A^{p^{-n}} = k^{p^{-n}}[x_1^{p^{-n}}, \cdots, x_r^{p^{-n}}]$$

is integral over $A$. (We're adjoining finitely many generators, each integral over $A$.) And $A^{p^{-n}}$ is the integral closure of $A$ in $K_n$. So $A \subset B \subset A^{-p^n}$. ○

## Chapter 5: Primary decomposition

We want to generalize unique prime decomposition in $\mathbb{Z}$ to Noetherian rings. We will show that every ideal is a unique intersection of primary ideals.

Definition 4.6. (5.1) An ideal is *primary* if, whenever $xy \in I$, then either $x \in I$ or there exists $n$ such that $y^n \in I$. (Equivalently, either $x \in I$ or $y \in \sqrt{I}$.)

For example, if $I$ is primary, then $\sqrt{I}$ is prime. The converse is usually false.

Lemma 4.7. *(5.2) If $\sqrt{I}$ is maximal, then $I$ is primary.*

*Proof.* Say $\sqrt{I} = M$. Then all elements of $M/I$ are nilpotent, and since it is a maximal ideal, it is equal to the nilradical.

$$M/I = \bigcap(\text{prime ideals } P/I) \subset P/I$$

$M$ is maximal, so $M/I$ is the unique prime ideal of $A/I$, and $M$ is the unique prime ideal containing $I$. Suppose $xy \in I$, and $x \notin I$. Set

$$J = \{z : xz \in I\}$$

Clearly, $I \subset J$ and $J$ is an ideal. $1 \notin I$, so $J \subset M$. So $y \in J \implies y \in M = \sqrt{I}$, so $y^n \in I$. ○

## Saturday optional class – October 13

The following fact, used in the proof of Corollary 4.4, warrants proof.

Proposition. If $A$ is a subring of $\mathbb{C}$, f.g. over $\mathbb{Z}$ then for all $x \in A$, $x \neq 0$, there is some maximal ideal $\mathfrak{m}$ of $A$ not containing $x$.

*Proof.* $A$ is a domain, f.g. over $\mathbb{Z}$. We want to prove $\bigcap \mathfrak{m} = 0$.

Take $K = \mathrm{Frac}(A)$. Suppose $0 \neq x \in \bigcap \mathfrak{m}$. Take $S = \{x^n\}$. Then $A \subset S^{-1}A = A[x^{-1}] \subset K$. If $S^{-1}A$ is not a field, then it has a maximal ideal, say $S^{-1}P \neq 0$ where $P \cap S = \emptyset$. (In $S^{-1}A$ every prime ideal comes from a prime of $A$.) So $x \notin P$. $P \neq 0, x \notin P$, so $P$ is not maximal.

Look at $B = A/P$. $B$ is not a field, because $P$ was not maximal. $\overline{x} = x \pmod P$, $\overline{x}$ is in every maximal ideal of $B$. Set $\overline{S} = \{\overline{x}^n\}$. Then $B \subset \overline{S}^{-1}B = B[x^{-1}] \subset \mathrm{Frac}(B)$. If $\overline{S}^{-1}B$ is not a field, it has a maximal ideal $\overline{S}^{-1}\overline{Q} \neq 0$. This contradicts $S^{-1}P$ being maximal. Therefore, $S^{-1}B$ is a field, hence $= \mathrm{Frac}(B)$. So $B \subset \overline{S}^{-1}B = B[\overline{x}^{-1}] = \mathrm{Frac}(B)$. So $B[x^{-1}]$ is finitely generated over $\mathbb{Z}$, and is a field, so is finite (since every $\mathbb{Z}[x_1, \cdots, x_n]/\mathfrak{m}$ is finite). So $B$ is finite and is a domain. But every finite domain is a field. This is a contrdiction. ○

The following fact was used in the proof of the Strong Nullstellensatz.

Proposition. If $0 \neq c \in k[X_1, \cdots, x_n] = A$ then there is a maximal ideal $M$ of $A$ that doesn't contain $c$.

*Proof.* $A$ is a domain f.g. over $k$, $0 \neq x \in A$. Then we need to show that $x \notin \bigcap \mathfrak{m}$.

Do the same thing. $S = \{x^n\}$. $A \subset S^{-1}A = A[x^{-1}] \subset K = \mathrm{Frac}(A)$. If $S^{-1}A$ is not a field, then it has a maximal ideal $S^{-1}P$, $P$ prime in $A$, with $x \notin P$. So $P$ is not maximal.

Keep going... you get $B = A/P$, with $k \subset B \subset B[\overline{x}^{-1}] = \mathrm{Frac}(B)$. So $\mathrm{Frac}(B)$ is a field, f.g. over a $k$-algebra. By the weak Nullstellensatz, it is finite over $k$. Then $B$ is integral over $k$, so is a field $\implies$ contradiction. ○

# Lecture 5: October 15

**Primary ideals.** Last time, we said that if $\sqrt{I}$ is maximal, then $I$ is primary. If $I$ is primary, then $\sqrt{I}$ is prime. But the converse is not true.

But, if things are Noetherian, if $P = \sqrt{I}$ then $P \supset I \supset P^n$ for some $n$. But $P^n$ can fail to be primary.

We will prove:

THEOREM 5.1. *(5.6) In a Noetherian ring, every ideal is a finite intersection of primary ideals.*

DEFINITION 5.2. An ideal $I$ is *irreducible* if $I$ cannot be written as $I = J_1 \cap J_2$ with each $J_i \supsetneq I$. Equivalently, whenever $I = J_1 \cap J_2$ then $J_1$ or $J_2 = I$.

LEMMA 5.3. *(5.4) In a Noetherian ring $A$, every ideal is a finite intersection of irreducible ideals.*

*Proof.* Suppose not: i.e. { ideals $I$ that are not finite ints. of irred. ideals} is nonempty. So it has a maximal element, say $I$. $I$ is not irreducible. So $I = J_1 \cap J_2$, with each $J_i \supsetneq I$. By maximality, each $J_i = \bigcap K_i$ and $J_2 = \bigcap L_j$ for $K$ and $L$ irreducible. So $I = \bigcap K_i \cap \bigcap L_j$. ○

LEMMA 5.4. *(5.5) In a Noetherian ring $A$, every irreducible ideal $I$ is primary.*

*Proof.* By passing to $A/I$, we may assume $I = 0$. We're assuming that (0) is irreducible; we need to show that it's primary. Suppose $xy = 0$. So we need to prove that $x = 0$ or $y^n = 0$ for some $n$. By the Noetherian property, the chain

$$\cdots \subset Ann(x^n) \subset Ann(x^{n+1}) \subset \cdots$$

(where $Ann(x) = \{a : ax = 0\}$) stabilizes. So at some point, $Ann(x^n) = Ann(x^{n+1})$. Suppose $a \in (x^n) \cap (y)$. Then $a = bx^n = cy$, and $ax = cyx = 0$, and $bx^{n+1} = cyx = 0$. So $b \in Ann(x^{n+1}) = Ann(x^n)$. So $bx^n = 0$ but also $bx^n = a$. So $a = 0$, and $(x^n) \cap (y) = 0$. But 0 is irreducible, so either $y = 0$ or $x^n = 0$. This is exactly what we wanted. ○

Putting together the previous two lemmas produces the Theorem.

COROLLARY 5.5. *(5.7) In a Noetherian ring, every radical ideal (i.e., one such that $I = \sqrt{I}$)* has a unique irredundant expression as a finite intersection of primes.

*Proof.* If $I$ is radical, then $I = \bigcap R_i$, with $R_i$ primary. Also $I = \sqrt{I} = \bigcap \sqrt{R_i}$. So $I = \bigcap P_i$, where $P_i = \sqrt{R_i}$.

Suppose $I = \bigcap P_i = \bigcap Q_j$ are two irredundant expressions. It suffices to show that each $P_i$ contains some $Q_j$. So suppose $P_i$ does not contain any $Q_j$. That is, for all $j$, there is some $x_j \in Q_j$ that is not in $P_i$. Then $\prod x_j \in \prod Q_j \subset \bigcap Q_j = \bigcap P_i \subset P_i$. But $P_i$ is prime, so some $x_j \in P_i$, a contradiction. So there exists a unique irredundant expression. ○

Recall: if $k = \overline{k}$, then subsets $V$ of $\mathbb{A}^n_k$ defined by polynomials correspond exactly to radical ideals $I$ of $A = k[X_1, \cdots, X_n]$, where $V \mapsto I(V) = \{f \in A : f(p) = 0 \ \forall p \in V\}$, and conversely $\{p \in \mathbb{A}^n_k : g(p) = 0 \ \forall g \in I\} \leftarrow I$.

Corollary 5.7 says that each $V$ has a unique irredundant expression $V = \bigcup V_i$, where $I(V_i)$ is prime, and $V_i$ is irreducible.

## Chapter 6: Artinian rings

Definition 5.6. A ring $A$ is *Artinian* (or *Artin*) if it satisfies the descending chain condition in ideals (every descending chain of ideals stabilizes). Equivalently, every nonempty set of ideals has a minimal element. *Later, we will also be talking about Artinian modules – modules that satisfy the descending chain condition on submodules.*

Our aim is to prove the following result:

Theorem 5.7.

$$\begin{aligned} \textit{Artinian} &\iff \textit{Noetherian + every prime is maximal} \\ &\iff \textit{Noetherian + every prime is maximal + only finitely many primes} \end{aligned}$$

Lemma 5.8. *(6.2) An Artinian domain is a field.*

*Proof.* Suppose $0 \neq x \in A$. Then

$$\cdots \supset (x^n) \supset (x^{n+1}) \supset \cdots$$

must terminate: $(x^n) = (x^{n+1})$ for some $n$. In particular, $x^n = x^{n+1} \cdot y$. But since we're in a domain, we can cancel the $x^n$. So $y$ is an inverse for $x$. ○

Corollary 5.9. *(6.3) In an Artinian ring, the prime ideals are maximal.*

Lemma 5.10. *(6.4) An Artinian ring has only finitely many prime ideals.*

*Proof.* It suffices to show that there are only finitely many maximal ideals. The set of ideals that are finite intersections of maximal ideals, is nonempty; so this set has a minimal element, say $I = \bigcap \mathfrak{m}_i$. Suppose $\mathfrak{m}$ is any maximal ideal. Then $\mathfrak{m} \cap I = I$ by the minimality of $I$, and so $\mathfrak{m} \supset \bigcap \mathfrak{m}_i$. By the earlier argument about $P_i$'s and $Q_j$'s (not even using maximality), $\mathfrak{m}$ contains one of the $\mathfrak{m}_i$'s. ○

Lemma 5.11. *(6.5) If $A$ is Artinian then $N = nil(A)$ is nilpotent. That is, $N^n = 0$ for some $n$.*

Note that you don't, a priori, know that $nil(A)$ is finitely generated.

*Proof.* The descending chain condition, applied to $\{N^n\}$, shows that $N^n = N^{n+r} =: I$ for some $n$ and all $r$. Suppose $I \neq 0$. Then $I \cdot I = I \neq 0$. Then

$$\{ \text{ ideals } J \,:\, J \subset I \text{ and } I \cdot J \neq 0\}$$

has a minimal element, say $J$. Then there is some $x \in J$ such that $x \cdot I \neq 0$. Then $J = (x)$ by minimality. Also $xI \cdot I = xI \neq 0$. So $xI \subset J$ and so $xI = J$ by minimality again. Therefore $x = xy$ for some $y \in I$. Since $I$ was defined to be a power of the nilradical, there exists $m$ such that $y^m = 0$. Then $x = xy = xy^2 = \cdots = xy^m = 0$. So $J = (x) = 0$, which is a contradiction. ○

# Lecture 6: October 17

RECALL we showed that Artinian (DCC on ideals) $\implies$ there are finitely many prime ideals, and all are maximal. Also, $\mathrm{nil}(A)$ is nilpotent.

Definition 6.1. For any ring $A$, an $A$-module $M$ is irreducible if its only submodules are 0 and $M$.

It is easy to see that the only irreducible $A$-modules are $A/\mathfrak{m}$ for maximal $\mathfrak{m}$.

Definition 6.2. An $A$-module $M$ has *finite length* if there is a chain

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M$$

with each $M_i/M_{i-1}$ irreducible.

Lemma 6.3. *(6.8)*

(1) *Given a submodule $M' \subset M$, $M$ has finite length iff $M'$ and $M/M'$ have finite length.*
(2) *Length, in the following sense, is well-defined. If*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M$$

*and*

$$0 = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_s = M$$

*are two chains with all $M_i/M_{i-1}$ and $N_j/N_{j-1}$ are irreducible, then $r = s$.*
*Define $\ell_A(M) = \ell(M)$ to be this number $r$, the* length *of $M$.*
(3) *If $M$ is of finite length and $M' \subset M$ then $\ell(M)$ is an additive function:*

$$\ell(M) = \ell(M') + \ell(M/M')$$

*Proof.* Standard exercise of Jordan-Hölder type. ○

Corollary 6.4. *If $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that $M_i/M_{i+1}$ has finite length for every $i$, then $M$ has finite length.*

*Proof.* Use induction on $n$, and Lemma 6.8(1). ○

Lemma 6.5. *For vector spaces over a field, TFAE:*

(1) *finite length;*
(2) *finite dimension;*
(3) *ascending chain condition on subspaces;*
(4) *descending chain condition on subspaces.*

*Proof.* Exercise. ○

Lemma 6.6. *(6.10) Assume $0 = \prod_1^n \mathfrak{m}_i$ (for some maximal ideals $\mathfrak{m}_i$) in a ring $A$. Then TFAE:*

(1) *$A$ is Noetherian;*
(2) *$A$ is Artinian;*

(3) *$A$ has finite length.*

So Artinian $\iff$ Noetherian and all the primes are maximal $\iff$ finite length. For example, $\mathbb{Z}/(p^n)$ is Artinian but not (if $n \geq 2$) a vector space over any field. Nonetheless, the "Artinian" condition should be *thought* of as being like a finite-dimensional vector space over a field.

*Proof.* *We will just prove* (1) $\iff$ (2)*; showing equivalence of* (3) *is similar.*

Say $0 = \prod_1^n \mathfrak{m}_i$. Define

$$M_j = \prod_1^j \mathfrak{m}_i \Big/ \prod_1^{j+1} \mathfrak{m}_i$$

This module is killed by the maximal ideal $\mathfrak{m}_{j+1}$. So $M_j$ is naturally an $A/\mathfrak{m}_{j+1}$-module (note $A/\mathfrak{m}_{j+1}$ is a field).

If $A$ is Noetherian, then each $M_j$ is a finitely-generated $A$-module, which implies that $M_j$ is finite dimensional as an $A/m_{j+1}$-vector space. This implies that $M_j$ has finite length, which in turn implies that $A$ has finite length as an $A$-module:

$$0 = \prod_1^n \mathfrak{m}_i \subset \prod_1^{n-1} \mathfrak{m}_i \subset \prod_1^{n-2} \mathfrak{m}_i \subset \ldots \subset \mathfrak{m}_1 \subset A$$

This implies the descending chain condition.

Conversely, if $A$ is Artinian then each $M_j$ is a vector space over $A/\mathfrak{m}_{j+1}$ with DCC, which implies that $M_j$ has finite dimension, hence finite length, which implies that $A$ has finite length. This implies ACC. ○

THEOREM 6.7. *(6.11) TFAE:*

(1) *$A$ is Artinian;*
(2) *$A$ is Noetherian and every prime ideal is maximal;*
(3) *$A$ is Noetherian, every prime ideal is maximal, and there exist only finitely many prime ideals.*

*Proof.* (1) $\implies$ (2): $A$ is Artinian; take $N = \mathrm{nil}(A)$. We know $N^n = 0$ for some $n$, and we also know that $N = \bigcap_1^r \mathfrak{m}_i$ (see Lemma 2.6), so $N = \bigcap \mathfrak{m}_i \supset \prod \mathfrak{m}_i$. So $\prod \mathfrak{m}_i^n = 0$. By Lemma 6.10, $A$ is Noetherian. We already know that all primes are maximal.

(2) $\implies$ (3): $\mathrm{nil}(A) = N$ *is a radical ideal* $\sqrt{0}$ *and so is an intersection of primes:*

$$N = \sqrt{0} = \bigcap_{i=1}^r P_i.$$

Suppose $P$ is any prime. $P \supset \bigcap P_i$. By an argument ("the argument with the $P_i$'s and $Q_j$'s"), $P$ contains some $P_i$. But $P_i$ is maximal, so $P = P_i$.

(3) $\implies$ (1):

$$N = \bigcap P_i = \bigcap \mathfrak{m}_i \supset \prod \mathfrak{m}_i$$

*If $R$ is Noetherian, then the nilradical is nilpotent, because there are finitely many generators, each of which is nilpotent.* So $0 = N^n \supset \prod \mathfrak{m}_i^n$. We are done, by Lemma 6.10. ○

THEOREM 6.8. *A ring $A$ is Artinian* $\iff$

$$A = \bigoplus_1^n \text{ Artinian local rings.}$$

*Proof.* Suppose $A$ is Artinian, with distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Then, as before,

$$\prod \mathfrak{m}_i \subset \bigcap \mathfrak{m}_i = N = \text{nil}(A)$$

so $\prod \mathfrak{m}_i^n = 0$ for some $n$.

CLAIM 6.9.

$$\mathfrak{m}_i^n + \prod_{j \neq i} \mathfrak{m}_j^n = A \tag{6.1}$$

*Proof of claim.* If not, then $\mathfrak{m}_i^n + \prod_{j \neq i} \mathfrak{m}_j^n \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. So $\mathfrak{m}_i^n \subset \mathfrak{m}$, and so $\mathfrak{m} = \mathfrak{m}_i$ *(primality of $\mathfrak{m}$ shows $\mathfrak{m}_i \subset \mathfrak{m}$)*. So $\prod_{j \neq i} \mathfrak{m}_j^n \subset \mathfrak{m}_i$. This is absurd: I can choose $x_j \in \mathfrak{m}_j - \mathfrak{m}_i$; then $\prod x_j^n \in \mathfrak{m}_i$ is a contradiction. ○

So $\mathfrak{m}_i^n + \bigcap_{j \neq i} \mathfrak{m}_j^n = A$ because the intersection contains the product.

Recall the Chinese Remainder Theorem: if $I_1, \ldots, I_r$ are ideals such that $I_i + \bigcap_{j \neq i} I_j = A$ for every $i$ ("the $I_i$ are coprime"), then there is a natural isomorphism

$$A/\bigcap_{i=1}^r I_i \xrightarrow{\cong} (A/I_1) \oplus \ldots \oplus (A/I_r)$$

and $\bigcap I_i = \prod I_i$.

Take $I_i = \mathfrak{m}_i^n$. Then $0 = \prod \mathfrak{m}_i^n = \bigcap \mathfrak{m}_i^n$. So

$$A = A/0 \cong A/\bigcap \mathfrak{m}_i^n = \prod_{i=1}^r (A/\mathfrak{m}_i^n)$$

*Showing that $A/\mathfrak{m}_j^n$ is local (i.e. that $\mathfrak{m}_j$ is the only maximal ideal): any other maximal ideal of $A/\mathfrak{m}_j^n$ would have the form $(\mathfrak{m}_i \cap \mathfrak{m}_j^n)/\mathfrak{m}_j^n$. Taking the quotient of 6.1 by $\mathfrak{m}_j^n$, we see that $A = \mathfrak{m}_i^n/\mathfrak{m}_j^n$; that is, $(\mathfrak{m}_i \cap \mathfrak{m}_j^n)/\mathfrak{m}_j^n$ is the whole ring $A/\mathfrak{m}_j^n$.*

The converse is "easy". ○

# Lecture 7: October 19

Lemma 7.1. *(6.16) Suppose $(A, \mathfrak{m}, k)$ is an Artinian local ring (i.e. $\mathfrak{m}$ is the unique maximal ideal and $k$ is the residue field). TFAE:*

(1) *every ideal $I$ in $A$ is principal;*
(2) *$\mathfrak{m}$ is principal;*
(3) *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$;*
(4) *every ideal is a power of $\mathfrak{m}$.*

(So this describes something that's like a PID, but it's not a domain.)

*Proof.* (1) $\implies$ (2) $\implies$ (3) are all clear.

(3) $\implies$ (1): If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$ then $\mathfrak{m} = \mathfrak{m}^2$, and then $\mathfrak{m} = 0$ by Nakayama's lemma. Suppose $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$. Pick any $x \in \mathfrak{m} - \mathfrak{m}^2$. Then $\mathfrak{m} = (x)$ again by Nakayama's lemma. Suppose $I \neq 0$. We know that $nil(A) = \mathfrak{m}$. For some $r$, $I \subset \mathfrak{m}^r$ but $I \not\subset \mathfrak{m}^{r+1}$. So there is some $y \in I$ such that $y = ax^r$, but $y \notin (x^{r+1})$. So $a \notin (x)$, so $a$ is a unit (in a local ring, anything not in the maximal ideal is a unit). Then $x^r \in I$, so $I = (x^r)$.

(1) $\implies$ (4) and (4) $\implies$ (3): easy exercises. ○

## Chapter 7: Dedekind domains

Definition 7.2. A *discrete rank 1 valuation* on a field $K$ is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that:

(1) $v(x) = \infty \iff x = 0$
(2) $v(xy) = v(x) + v(y)$ (where $\infty +$ anything $= \infty$)
(3) $v(x + y) \geq \min\{v(x), v(y)\}$.

Example 7.3.

(1) Take $K = \mathbb{Q}$, $p$ a fixed prime, and define $v(\frac{a}{b} \cdot p^n) = n$ when $a, b$ are prime to $p$.
(2) $K$ is the field of meromorphic functions on a Riemann surface $X$, $p \in X$. Then define $v(f)$ to be the order of vanishing of $f$ at $p$.
(3) $K$ is the field of rational functions on a curve $X$ over a field $k$, $p \in X$ where $X$ is smooth. Then define $v(f)$ is the order of vanishing of $f$ at $p$.

Definition 7.4. Given $v$, the valuation ring is

$$\mathcal{O}_v = \{x \in K \,:\, v(x) \geq 0\}$$

This has a unique maximal ideal

$$\mathfrak{m}_v = \{x \in K \,:\, v(x) > 0\}$$

We will only discuss valuations that are discrete and of rank 1. So in the future "valuations" will mean discrete rank 1 valuations.

Definition 7.5. A discrete valuation ring (DVR) is any ring of the form $\mathcal{O}_v$.

LEMMA 7.6. *(7.4) If $A$ is a DVR, then $A$ is a local Noetherian domain in which every nonzero ideal is a power of the maximal ideal, and is principal. (So it's a local ring that's a PID.)*

*Proof.* Suppose $A = \mathcal{O}_v$, and $I$ is a nonzero ideal. If $x \in I$ with $v(x) = 0$ then $I = A$: anything of valuation 0 is a unit, since $v(x) = 0 \implies v(x^{-1}) = 0$. Take $n = \min\{v(x) : x \in I\} > 0$. Choose $x \in I$ such that $v(x) = n$. Suppose $y \in I$; then $v(y) \geq n$. So $v(\frac{y}{x}) \geq 0$, so $\frac{y}{x} \in \mathcal{O}_v$; $y \in (x)$ so $I \subset (x)$. In particular, $\mathfrak{m}$ is principal.

Say $\mathfrak{m} = (z)$. Since $v(\mathfrak{m})$ is a subgroup of $\mathbb{Z}$, say $r\mathbb{Z}$, it is easy to check that $v(z) = r$. Then $n = rs$; verify that $I = \mathfrak{m}^s$. ○

LEMMA 7.7. *(7.5) If $A$ is a domain, then $A = \bigcap A_P = \bigcap A_{\mathfrak{m}}$ inside $Frac(A)$.*

*Proof.* Exercise. ○

LEMMA 7.8. *(7.6) Suppose $A$ is a domain. Then $A$ is normal iff every localization $A_P$ is normal.*

*Proof.* Exercise. ○

LEMMA 7.9 (Part of Chinese Remainder Theorem). *(7.7) If $J_1, \cdots, J_r$ are coprime ideals (i.e. $J_i + (\bigcap_{j \neq i} J_j) = A$) then*

$$\bigcap_{i=1}^{r} J_i = \prod_{i=1}^{r} J_i$$

*(It also suffices to assume instead that $J_i + J_j = A$ for all $i \neq j$.)*

*Proof.* Exercise. ○

Now assume that $(A, \mathfrak{m}, k)$ is a Noetherian local domain, $Frac(A) = K$, and that $\mathfrak{m}$ is the unique nonzero prime ideal.

LEMMA 7.10. *(7.8) Every $I \neq 0$ is $\mathfrak{m}$-primary and contains a power of $\mathfrak{m}$.*

*Proof.* $I$ is $\mathfrak{m}$-primary because $\sqrt{I} = \mathfrak{m}$. *The second half follows from Lemma 7.11 below.* ○

LEMMA 7.11. *Every ideal in a Noetherian ring contains a power of its radical.*

*Proof.* Because the ring is Noetherian, $\sqrt{I}$ is finitely-generated, say by $x_1, \cdots, x_r$. Then for every $i$ there is some $n_i$ such that $x_i^{n_i} \in I$. Check that $(a_1 x_1 + \cdots + a_r x_r)^N \in I$ for sufficiently large $I$. ○

LEMMA 7.12. *(7.9)*

$$\mathfrak{m}^r \neq \mathfrak{m}^{r+1}$$

*Proof.* Nakayama's lemma. ○

PROPOSITION 7.13. *(7.10) (Under assumed conditions) TFAE:*

(1) *$A$ is a DVR;*
(2) *$A$ is normal;*
(3) *$\mathfrak{m}$ is principal;*
(4) *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$;*
(5) *every $I \neq 0$ is a power of $\mathfrak{m}$;*
(6) *there exists $x \in A$ such that every nonzero ideal $I$ is a prime of $(x)$.*

(The significance here is that normal is usually much weaker than all the other conditions.)

*Proof.* (1) $\implies$ (2): Suppose $z \in K$ is integral over $A$, say $z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0$ for $a_i \in A$. We need to show that $z \in A$. If $v(z) < 0$ then $v(a_i z^i) > v(z^n)$ for all $i \leq n-1$ and

$$v(z^n + a_{n-1}z^{n-1} + \cdots + a_0) = n \cdot v(z) \neq v(0) = \infty$$

is a contradiction.

(2) $\implies$ (3): Suppose $0 \neq a \in \mathfrak{m}$. Then $\mathfrak{m}^n \subset (a)$, $\mathfrak{m}^{n-1} \not\subset (a)$ for some $n$ (because $(a)$ is $\mathfrak{m}$-primary). Choose $b \in \mathfrak{m}^{n-1}$ that is not in $(a)$, and $x = \frac{a}{b} \in K$. Then $x^{-1} \notin A$ and so is not integral over $A$. Then taking $M = \mathfrak{m}$ in Proposition 3.4(4) (equivalent definitions of being integral), we have that $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$. But $x^{-1}\mathfrak{m} \subset A$, by construction. So $x^{-1}\mathfrak{m} = A$ and $\mathfrak{m} = (x)$.

(3) $\implies$ (4): Obvious (since $\mathfrak{m} \neq \mathfrak{m}^2$).

(4) $\implies$ (5): Suppose $0 \neq I \neq A$. By Lemma 7.8, there is some $n$ such that $I \supset \mathfrak{m}^n$. By Lemma 6.11, $A/\mathfrak{m}^n$ is Artinian. By Lemma 6.16 applied to $A/\mathfrak{m}^n$, we have $I/\mathfrak{m}^n = \mathfrak{m}^r/\mathfrak{m}^n$ for some $r$; by Nakayama's lemma, $I = \mathfrak{m}^r$.

(5) $\implies$ (6): There is some $x \in \mathfrak{m} - \mathfrak{m}^2$. Then $(x) = \mathfrak{m}^r$ and then $r = 1$.

(6) $\implies$ (1): $(x^r) \neq (x^{r+1})$. So for all $a \in A - \{0\}$, there is a unique $r$ such that $(a) = (x^r)$. Then define $v$ by $v(a) = r$, and extend $v$ to $K^*$ by

$$v\left(\tfrac{a}{b}\right) = v(a) - v(b)$$

which is well-defined. ○

## SATURDAY OPTIONAL LECTURE – OCTOBER 20

**Regularity, free resolutions, and sheaves.** Let $(A, \mathfrak{m}, k)$ be a local ring of maximal ideal $\mathfrak{m}$. Take generators $x_1, \cdots, x_n$ of an $A$-module $M$, and let $F_0$ be the free module on the $x_i$. So we construct a map $F_0 \to M \to 0$, and taking the kernel, we get a short exact

sequence

$$0 \to K \to F_0 \to M \to 0$$

Now play the same game with the kernel: let $F_1$ be the free module on the generators of $K$, and construct

$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$

which is an exact sequence. There is nothing canonical about this. Either the kernel will be free (in which case we stop), or the chain is infinite. This is called a *free resolution.*

THEOREM. $A$ is regular $\iff$ for every $A$-module $M$, any construction of a free resolution terminates in finitely many steps, $\iff$ for the module $k$, every free resolution terminates, $\iff$ $k$ has a finite free resolution.

THEOREM. A regular local ring is a UFD.

LEMMA. If $A$ is regular, then $A_P$ is regular for all $P$.

*Proof of lemma.* $A/P$ has a free resolution

$$0 \to F_r \to \cdots \to F_0 \to A/P \to 0$$

because $A$ is regular. Now localize:

$$0 \to (F_r)_P \to \cdots \to (F_0)_P \to (A/P)_P = k \to 0$$

since localizing preserves exactness. Every $(F_i)_P$ is a free $A_P$-module. So $A_P$ is a local ring whose residue field has a finite free resolution. By Theorem regularity, $A_P$ is regular. ○

*Proof of theorem.* Assume $A$ is regular.

Assume $\dim A \geq 2$, since otherwise it's a DVR, hence PID. We need to show that every height 1 prime $P$ is principal. Let $X = \operatorname{Spec} A$, and $U = X - \{\mathfrak{m}\}$. $U$ is not an affine scheme. All the local rings of $U$ are the rings $A_P$, for $P \neq \mathfrak{m}$. All of them have dimension $< \dim A$. By induction, all local rings of $U$ are unique factorization domains.

It is quite easy to see that $A$ is normal, because regular is equivalent to:

$$Gr_m(A) = \bigoplus_{n=0}^{\infty} (\mathfrak{m}^n/\mathfrak{m}^{n+1}) \cong k[x_1, \cdots, x_d]$$

and it is easy to show that $A$ is normal whenever $Gr_m(A)$ is normal. So, $A$ has a class group $Cl(A)$. Because all the local rings of $U$ are UFD's, $Cl(A) = Pic(A)$, the group of isomorphism classes of invertible sheaves on $U$, under $\otimes$. We need to show that $Pic(U)$ is trivial.

$Cl(A)$ is generated by the height 1 primes. The isomorphism $\varphi : Cl(A) \to Pic(U)$ takes $P \mapsto \mathcal{O}(P)$. The coherent sheaves on the affine scheme $X$ are the finitely-generated modules over $A$. So here, $P \to \widetilde{P}$ (the sheaf in Spec $A$ associated to $P$), and $\widetilde{P} \mapsto \mathcal{O}(P) = \widetilde{P}|_U$. Now take a finite free resolution of $P$:

$$0 \to F_r \to \cdots \to F_0 \to P \to 0$$

where the $F_i$'s are free $A$-modules.

Turn these modules into sheaves on $X$, and restrict to $U$. (A free module turns into a free sheaf, and the restriction of a free sheaf is also free.)

$$0 \to \mathcal{F}_r \to \cdots \to \mathcal{F}_0 \to \mathcal{O}(P) \to 0$$

where $\mathcal{F} \cong \mathcal{O}_U^{\oplus n_i}$. $\mathcal{O}(P)$ is invertible in $U$, and "invertible" is the same as "locally free of rank 1."

Now take the determinant of the LES above. The alternating product of determinants is trivial:

$$\det \mathcal{O}(P) \otimes (\det \mathcal{F}_0)^{-1} \otimes (\det \mathcal{F}_1) \otimes \cdots \otimes (\det \mathcal{F}_r)^{-r} = \text{ trivial sheaf on } U$$

Since $\mathcal{F}_i$ is free, $\det \mathcal{F}_i \cong \mathcal{O}_U$ is trivial. So $\mathcal{O}(P) \cong \det \mathcal{O}(P)$, and so $\det \mathcal{O}(P) \cong \mathcal{O}_U$. ○

"I'm still doing algebra... I'm just broadening my definition of what algebra is."

Suppose $X \hookrightarrow \mathbb{A}_k^n$ has dimension $d$. There is a projection $\mathbb{A}_k^n \to \mathbb{A}_k^d$. Then there is a linear projection $\pi$ such that $\pi|_X$ is finite. Saying that the morphism is finite is stronger than saying that the fibers are finite. For example, $\mathbb{A}^1 - \{0\} \hookrightarrow \mathbb{A}^1$ induces a map $k[X, X^{-1}] \leftarrow k[X]$ of functions. This has finite fibers, but isn't a finite morphism.

The problem is that it isn't proper: in the manifold world, "proper" means that the inverse image of a compact set is compact. In the algebraic context, the inverse image of a compact set is almost always quasicompact. So instead, we say that $\pi : X \to Y$ is *proper* if $\pi$ is of finite type and separated, and for all schemes $Z \to Y$, the morphisms $X \times_Y Z \xrightarrow{\pi_Z} Z$ takes closed sets to closed sets. We say that $\pi$ is "universally closed".

# Lecture 8: October 22

RECALL we had a local Noetherian domain $(A, \mathfrak{m}, k)$, where $\mathfrak{m}$ is the unique nonzero prime ideal (so $\dim A = 1$). We showed that $A$ is a DVR $\iff$ $A$ is normal. Today, $A$ will be a Noetherian domain (not necessarily local) in which every nonzero prime ideal is maximal.

Lemma 8.1. *(7.11) Every nonzero ideal $I$ is uniquely a product $I = \prod Q_i$, where $Q_i$ is primary and $\sqrt{Q_i} \neq \sqrt{Q_j}$.*

*Proof.* We'll need the Chinese Remainder Theorem, but in a stronger form than originally stated. If $I_1, \cdots, I_n$ are ideals that are pairwise coprime (i.e. $I_i + I_j = A$ whenever $i \neq j$) then $\bigcap I_i = \prod I_i$ and there is an isomorphism

$$A/\bigcap I_i \xrightarrow{\cong} (A/I_1) \times \cdots \times (A/I_n).$$

We know that $I$ has a decomposition $I = \bigcap Q_i$ where $Q_i$ are primary. *By the Chinese remainder theorem, it suffices to show that the $Q_i$'s are pairwise coprime.*

*First we show that this hypothesis is satisfied when $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$. By Lemma 7.10, $Q_i \supset \mathfrak{m}_i^r$ and $Q_j \supset \mathfrak{m}_j^s$ where $\mathfrak{m}_i = \sqrt{Q_i}$ and $\mathfrak{m}_j = \sqrt{Q_j}$ are different maximal ideals. Then $\mathfrak{m}_i + \mathfrak{m}_j = A$, so we can find $a_i \in \mathfrak{m}_i$ and $a_j \in \mathfrak{m}_j$ such that $a_i + a_j = 1$. But I claim that $\mathfrak{m}_i^r + \mathfrak{m}_j^s = A$ as well, because $1 = (a_i + a_j)^{2\max\{r,s\}}$ has an expansion with each term in $\mathfrak{m}_i^r$ or $\mathfrak{m}_j^s$. This shows that $Q_i + Q_j = A$.*

Now suppose $\sqrt{Q_i} = \sqrt{Q_j}$. Since $\dim A = 1$, $Q_i \cap Q_j$ is also primary. *Suppose $xy \in Q_i \cap Q_j$. Assume $x \notin Q_i \cap Q_j$ and WLOG $x \notin Q_i$. Then $y^n \in Q_i$ and $y^m \in Q_j$ because they have the same radical. So $y^{\max\{m,n\}} \in Q_i \cap Q_j$.* Furthermore, $\sqrt{Q_i \cap Q_j} = \sqrt{Q_i} = \sqrt{Q_j}$. *Since $Q_i \cap Q_j$ is primary, the radical is prime, contained in $\sqrt{Q_i}$ so it must be $\sqrt{Q_i}$.*

**Uniqueness:** Suppose $I = \prod_{i=1}^r Q_i = \prod_{j=1}^s \widetilde{Q_j}$. Then $\bigcap Q_i = \bigcap \widetilde{Q}_j$. Then by an argument we've seen before, the sets $\{\sqrt{Q_i}\}$ and $\{\sqrt{\widetilde{Q}_j}\}$ are the same (up to reordering).

Suppose $x_r \in Q_r - \widetilde{Q_r}$. For $i < r$ pick $x_i \in Q_i - \sqrt{Q_r}$. Then $\prod_1^{r-1} x_i \notin \sqrt{Q_r}$ and $\prod_1^r x_i \in \prod_1^r Q_i = I \subset \widetilde{Q}_r = (\prod_1^{r-1} x_i) \cdot x_r$. No power of $\prod_1^{r-1} x_i$ lies in $\widetilde{Q}_r$, so $x_r \in \widetilde{Q}_r$. ○

THEOREM 8.2. *(7.12) For a Noetherian domain $A$* of dimension 1, TFAE:

(1) $A$ is normal;
(2) every $A_P$ is a DVR (if $P$ is a nonzero prime);
(3) every primary ideal is a power of a prime ideal.

*Proof.* (1) $\iff$ (2): This is 7.10.

(2) $\implies$ (3): Suppose $Q$ is $P$-primary. Then $Q_P = (P_P)^r$ for some $r$ (in a DVR, every nonzero ideal is a power of $\mathfrak{m}$, and now $(P_P)$ is the unique maximal ideal). Let $x \in Q$. Then $x \in (P_P)^r$. There exists $s \notin P$, $a \in P^r$ such that $x = \frac{a}{s}$. Then $sx = a \in P^r$. $s \notin P$ so $x \in P^r$ (any power of a maximal ideal is primary). So $Q \subset P^r$. You can prove that $P^r \subset Q$ by a similar argument.

(3) $\implies$ (2): Every nonzero ideal $I$ of $A_P$ is $P_P$-primary, so $I = Q_P$ for some $P$-primary $Q$. But $Q = P^r$, so $I = P_P^r$. Done by 7.10. ○

DEFINITION 8.3. A *Dedekind domain* is a Noetherian domain in which every nonzero prime ideal is maximal, and which is not a field.

THEOREM 8.4. *(7.14)*

(1) *Suppose $A$ is a Noetherian domain, that is not a field. Then $A$ is Dedekind iff $A_P$ is a DVR for all nonzero primes $P$. (Note that both of these conditions imply 1-dimensionality, though that isn't explicitly stated.)*
(2) *In a Dedekind domain, every nonzero ideal is uniquely a product of prime ideals.*

Definition 8.5. Let $A$ be a Noetherian domain, and let $K = Frac(A)$. Then a *fractional ideal* of $A$ is a nonzero, finitely generated sub-$A$-module of $K$.

Theorem 8.6. *(7.16) If $A$ is Dedekind then the fractional ideals form a group under multiplication. It is the free abelian group on the set of nonzero prime ideals of $A$.*

*(You need a Dedekind domain in order to have inverses.)*

This is a restatement of unique factorization.

*Proof.* Suppose $I$ is fractional. Define

$$I^{-1} = \{a \in K \,:\, x \cdot I \subset A\}$$

We need to show that $I \cdot I^{-1} = A$. Let $J = I \cdot I^{-1}$. By construction, $J \subset A$. Fix a nonzero prime $P$. Then $I_P = (P_P)^r$ for some $r \in \mathbb{Z}$.

Observe: in a DVR, the ideals are powers of maximal ideals, so the fractional ideals are the integral powers of the maximal ideals ($\mathfrak{m}^r$ for $r \in \mathbb{Z}$). Claim that $I = \mathfrak{m}^r$ where $r = \min\{v(x) \,:\, x \in I\}$.

Then $(I^{-1})_P = (I_P)^{-1} = (P_P)^{-r}$. So $J_P = A_P$. *Since $A$ is the intersection of its localizations, $A = J$.* ○

Since $I$ is fractional, finite generation of $I$ implies that there is some $x \neq 0$ in $A$ such that $I \supset x \cdot A$. Then $I^{-1} \subset x^{-1}A$, which shows that $I^{-1}$ is finitely-generated.

Definition 8.7. $I$ is principal if $I = x \cdot A$ for nonzero $x \in K$. The principal ideals form a subgroup of the group of all ideals. The quotient group is the *class group* of $A$.

Theorem from number theory: if $A$ is the ring of integers in a number field, then the class group is finite. In algebraic geometry, for curves $C$ over a field $k$, there is a map

$$0 \to Cl^0 \to Cl \xrightarrow{deg} \mathbb{Z}$$

where $Cl^0$ is the group of $k$-points on an algebraic variety, the Jacobian of $C$, and the dimension of the Jacobian is the genus.

## Chapter 8: Gradings and filtrations

Definition 8.8. A ring $A$ is *graded* if

$$A = \bigoplus_{n \geq 0} A_n$$

where $A_m$ is a subgroup of $A$ under addition, and the multiplication takes $A_m A_n \hookrightarrow A_{m+n}$. So $A_0$ is a ring, and every $A_n$ is an $A_0$-module.

We say that $A_n$ is the set of elements of degree $n$.

EXAMPLE 8.9. $A = k[X_1, \cdots, X_r]$, where $k = A_0$, and $\deg X_i = 1$.

# LECTURE 9: OCTOBER 24

RECALL we had a graded ring $A = \bigoplus_{n \geq 0} A_n$.

PROPOSITION 9.1. *(8.2) $A$ is Noetherian $\iff$ $A_0$ is Noetherian and $A$ is finitely generated as an $A_0$-algebra.*

*Proof.* ( $\Longleftarrow$ ) is the Hilbert Basis theorem.

( $\Longrightarrow$ ) $I := \bigoplus_{n \geq 1} A_n$ is an ideal in $A$, and $A_0 = A/I$. If $A$ is Noetherian then so is $A_0$, and $I$ is finitely generated as an ideal. So pick generators $f_1, \cdots, f_r$. We may assume that each $f_i$ is homogeneous (otherwise you just break them up into homogeneous pieces, and the pieces will be in $I$ by definition of $I$); say $f_i \in A_{d_i}$.

It suffices to prove that $A = A_0[f_1, \cdots, f_r]$. Clearly $A \supset A_0[f_1, \cdots, f_r]$. If $x' \in A$ then $x' = x_0 + x$, where $x_0 \in A_0$ and $x \in I$. Then $x = \sum h_i f_i$. By induction on the degree, each $h_i \in A_0[f_1, \cdots, f_r]$. Then $x \in A_0[f_1, \cdots, f_r]$. ○

DEFINITION 9.2. If $R = \bigoplus_{n \geq 0} R_n$ is a graded ring, then $M$ is a *graded $R$-module* if $M = \bigoplus_{n \geq 0} M_n$ and $R_m \cdot M_n \subset M_{m+n}$.

Now fix a Noetherian ring $A$ (not graded), and an ideal $I$.

DEFINITION 9.3. An $I$-filtration of $M$ is a descending chain

$$M = M_0 \supset \cdots \supset M_n \supset M_{n+1} \supset \cdots$$

of submodules of $M$ such that $IM_n \subset M_{n+1}$ for all $n$. The filtration is *stable* if $IM_n = M_{n+1}$ for all $n$ sufficiently large.

For example, $M_n = I^n M$ is a stable filtration.

Two $I$-filtrations $(M_n)$ and $(M'_n)$ are equivalent if for all $n$, there is some $p, q$ such that $M_n \supset M'_{n+p}$ and $M'_n \supset M_{n+q}$.

LEMMA 9.4. *(8.4) If $(M_n)$ and $(M'_n)$ are stable, they have bounded difference: there exists $m$ such that $M_{n+m} \subset M'_n$, and $M'_{n+m} \subset M_n$, for all $n$.*

*Proof.* It is enough to take $M'_n = I^n M$. Then $I^n M \subset M_n$. Also, there exists $m$ such that $IM_n = M_{n+1}$ for all $n \geq m$. Then $M_{n+m} = I^n M_m \subset I^n M$. ○

Define $A^* = \bigoplus_{n \geq 0} I^n$; this is Noetherian by Proposition 8.2: it's Noetherian in degree zero, and it is generated by its elements of degree 1. (We only need finitely many generators

because $I$ is finitely generated, since $A$ is Noetherian.) Fix an $I$-filtration $(M_n)$ of $M$, so

$$M^* = \bigoplus_{n \geq 0} M_n$$

is a graded $A^*$-module.

LEMMA 9.5. *(8.5) $M^*$ is a finite $A^*$-module iff the filtration $(M_n)$ is stable.*

*Proof.* ( $\Longleftarrow$ ) Suppose $IM^n = M_{n+1}$ for all $n \geq n_0$. Pick finitely many generators $m_{ij}$ of $M_i$ for all $i \leq n_0$. So $\{m_{ij}\}$ is finite. It's an easy exercise to show that the $\{m_{ij}\}$ generate $M^*$.

( $\Longrightarrow$ ) Assume $M^*$ is generated by $\{m_k\}$. As before, we can assume the $m_k$ are homogeneous, because otherwise you could just break them into homogeneous pieces; say each $m_k$ has degree $n_k$. Define $n_0 = \max\{n_k\}$. Then $IM_n = M_{n+1}$ for all $n \geq n_0$. ○

COROLLARY 9.6. *(8.6) Suppose $N \subset M$ is a submodule. Assume $(M_n)$ is a stable $I$-filtration of $M$. Then $(N \cap M_n)$ is a stable $I$-filtration of $N$.*

*Proof.* $N^*$ is a sub-$A^*$-module of $M^*$; we are done by the fact that $A^*$ is Noetherian, and $N^*$ is an $A^*$-module. ○

COROLLARY 9.7. *(8.7) Given $N \subset M$ there are some $k$ such that*

$$(I^n M) \cap N = I^{n-k}((I^k M) \cap N)$$

*for all $n \geq k$.*

*Proof.* Take Corollary 8.6 with $M_n = I^n M$. ○

Corollary 8.6 and Corollary 8.7 are collectively often called the Artin-Rees lemma.

THEOREM 9.8. *(8.8)*

$$N := \bigcap_{n \geq 0} I^n M = \{x \in M \,:\, x \text{ is killed by some element of } 1 + I\}$$

*Proof.* There exists $k$ such that

$$(I^n M) \cap N = I^{n-k}((I^k M) \cap N)$$

for all $n \geq k$. Then $N = I^{n-k}N$, because LHS $= N = ((I^k M) \cap N)$, by definition of $N$. In particular, $N = IN$. Apply Cayley-Hamilton with $\varphi = 1$, to see that here exists $a_0, \cdots, a_{n-1} \in I$ with the property that

$$(1 + \sum a_i)N = 0$$

Conversely, if $(1 - a)x = 0$, for $a \in I$, $x \in M$, then $x = a^n x$ for all $n$, and so $x \in \bigcap I^n M$. ○

In particular, if $A$ is local and $I = \mathfrak{m}$, then $\bigcap \mathfrak{m}^n M = 0$ (since $1 + \mathfrak{m}$ consists of units). It's like saying that any function whose Taylor series vanishes, is zero. This emphasizes the fact that we're in the algebraic, Noetherian world, not the differentiable one.

COROLLARY 9.9 (Krull's theorem). *(8.9) If $A$ is a domain, and $I \neq A$, then $\bigcap I^n = 0$. (E.g. if $A$ is the coordinate ring of an affine variety, then the only function that vanishes to all orders is the zero function)*

**Dimension.** Suppose $A_0$ is Artinian, and $A = A_0[x_1, \cdots, x_s]$ is a graded $A_0$-algebra with each $x_i$ homogeneous of degree $k_i > 0$. Let $I = \bigoplus_{n \geq 1} A_n$ be the *irrelevant ideal*. (In projective algebraic geometry, this is the most significant ideal that does not correspond to a point on the variety.) Note that $A/I = A_0$. Let $M$ be a finitely-generated graded $A$-module. Note that $M_r = \bigoplus_{n \geq r} M_n / \bigoplus_{n \geq r+1} M_n$ so is killed by $I$. So $M_r$ is a Noetherian (in particular, finitely generated) $A_0$-module. Since $A_0$ is Artinian it has finite length $\ell(M_r)$.

Define the *Poincaré series*

$$P(M, t) = \sum_{r \geq 0} \ell(M_r) t^r \in \mathbb{Z}[[t]]$$

THEOREM 9.10. *(9.1) There exists $f(t) \in \mathbb{Z}[t]$ such that*

$$P(M, t) = \frac{f(t)}{\prod_{i=1}^{s} (1 - t^{k_i})}$$

*and $s$ is the number of generators of $A$ as an $A_0$-algebra.*

*Proof.* By induction on $s$, the number of generators. If $s = 0$ then $P(M, t) \in \mathbb{Z}[t]$ (there are only finitely many $M_n$). *What is the highest degree thing you can get via linear combinations of generators $f_i$ of $M$, and coefficients in $A = A_0$? Everything in $A_0$ has degree 0, so multiplying by $a \in A_0$ isn't going to raise the degree. So you can't get a higher degree element than the $f_i$ of highest degree. Therefore, $M_n = 0$ for large enough $n$.*

Assume $s > 0$ and the obvious induction hypothesis. Let

$$B := A/(x_s) = A_0[x_1, \cdots, x_{s-1}]$$

By the induction hypothesis, the theorem is true for all $B$-modules.

Define $K \subset M$ to be the "things annihilated by $x_s$" (kernel of multiplication by $x_s$), and $L$ to be the cokernel. We have an exact sequence

$$0 \to K \to M \xrightarrow{x_s} M \to L \to 0$$

and we can break this into exact pieces

$$0 \to K_n \to M_n \xrightarrow{x_s} M_{n+k_s} \to L_{n+k_s} \to 0$$

Length is an additive function, i.e. $\ell(K_n) + \ell(M_{n+k_s}) = \ell(M_n) + \ell(L_{n+k_s})$. We can multiply by $t^{n+k_s}$ and sum over $n$:

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

where $g(t)$ is a polynomial. Since $K$ and $L$ are $B$-modules of smaller dimension, apply the induction hypothesis. We are done because $P(L,t)$ and $P(K,t)$ have the correct shape. ○

Scholium 9.11 (Corollary of the proof of 9.1). (9.3) If $x \in A$ is homogeneous of degree $\geq 1$, and $x$ is not a zero-divisor in $M$, then $d(M/xM) = d(M) - 1$.

*Proof.* Replace $x_s$ by $x$ in the proof of 9.1. Then $K = 0$; run through the argument again. *If $x$ lives in degree $k$, you get*

$$\ell(M_{n+k}) = \ell(M_n) + \ell(L_{n+k})$$
$$P(M,t) - \sum_{i=0}^{k-1} \ell(M_i)t^i = t^k P(M,t) + P(L,t) - \sum_{i=0}^{k} \ell(L_i)t^i$$
$$(1-t^k)P(M,t) = P(L,t) + \sum \left(\ell(M_i) - \ell(L_i)\right) t^i$$

*but the last term is zero: the image of multiplication by $x$ has degrees $\geq k$, so $M_i = L_i$ for $i < k$. Take $\mathrm{ord}_{1-t^k}$ of both sides of the above: $1 + d(M) = d(L)$.* ○

# Lecture 10: October 26

Let $A = \bigoplus_{n\geq 0} A_n$ be graded, $A_0$ Artinian, and $A$ Noetherian (equivalently, it is a finitely generated $A_0$-algebra). Suppose $A$ has generators $x_1, \cdots, x_s$ where $x_i$ has degree $k_i$. Let $M = \bigoplus M_n$ be a finitely generated graded $A$-module. So each $M_n$ is a finitely generated $A_0$-module, and $\ell(M_n)$ is finite. We defined

$$P(M,t) = \sum \ell(M_n)t^n \in \mathbb{Z}[[t]]$$

and proved that

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$$

where $f(t) \in \mathbb{Z}[t]$. Denote by $d(M)$ the order of the pole at $t = 1$ of $P(M,t)$.

Corollary 10.1. *(9.2) If each $k_i = 1$, then there is some polynomial $p(t) \in \mathbb{Q}[t]$ of degree $d(M) - 1$ such that $p(n) = \ell(M_n)$ for sufficiently large $n$.*

*Proof.* $\ell(M_n)$ is the coefficient of $t^n$ in $f(t) \cdot (1-t)^{-s}$ by definition of $P$. Cancel powers of $(1-t)$, then assume $d := d(M) = s$ and $f(1) \neq 0$. Say $f(t) = \sum_{k=0}^{N} a_k t^k$. Then because

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k$$

we calculate

$$\sum \ell(M_n)t^n = \sum_{k=0}^{N} a_k t^k \cdot (1-t)^{-d} = \sum_{0}^{N} a_k t^k \sum_{m=0}^{\infty} \binom{d+m-1}{d-1} t^m$$

So $\ell(M_n) = \sum_{k+m=n} a_k \binom{d+m-1}{d-1}$, and the RHS is a polynomial in $n$ with leading coefficient $\sum_{k=0}^{N} \frac{a_k}{(d-1)!}$ *and degree* $d-1$. *Why:*

CLAIM 10.2. *$c_n\binom{t}{n}$ is a polynomial of degree $n$ in $t$.*

*Proof.* This looks like $c_n \frac{t!}{n!(t-n)!} = \frac{c_n}{n!}\frac{t!}{(t-n)!}$. If $n = 0$, this is a constant; if $n = 1$, this is $const \cdot t$, and in general, this is $\frac{c_n}{n!} \cdot t(t-1)(t-2)\cdots(t-n+1)$, a polynomial of degree $n$. □*(Claim)*

*There are only finitely many $k$'s ($N+1$ of them). So there are $\min\{n+1, N+1\}$ terms in $\sum_{k+m=n} *$. By the claim each term $a_k\binom{d+m-1}{d-1} = a_k\binom{d+n-k-1}{d-1}$ is a polynomial in $n$ (for each $k$) of degree $d-1$, and if $n \geq N$ then the number of such terms has nothing to do with $n$. So you're adding together a fixed number of polynomials in $n$ of degree $d-1$, which gives a polynomial in $n$ of degree $\leq d-1$.* ○

**The associated graded ring.** Now, fix a local Noetherian ring $(A, \mathfrak{m}, k)$, a finitely-generated $A$-module $M$, and an $\mathfrak{m}$-primary ideal $Q$. (These things are all un-graded.)

Define

$$G_Q(A) = \bigoplus_{n\geq 0} Q^n/Q^{n+1} =: \bigoplus A_n$$

(a quotient of $A^* = \bigoplus_{n\geq 0} Q^n$).

CLAIM 10.3. *$A_0 = A/Q$ is Artinian.*

*Proof. By Lemma 6.11, it suffices to show that all primes are maximal. We will show that $\overline{\mathfrak{m}}$ is the only prime in $A/Q$. That is, we need to show that there is no prime between $Q$ and $\mathfrak{m}$ in $A$. So suppose $Q \subset P \subset \mathfrak{m}$. Then $\mathfrak{m} = \sqrt{Q} \subset \sqrt{P} = P \subset \mathfrak{m}$, which forces $P = \mathfrak{m}$.* ○

CLAIM 10.4. *$G_Q(A)$ is generated over $A_0$ by the degree-2 elements $Q/Q^2$.*

*Proof. The degree-0 elements are just elements of $A/Q$, and a typical element of $G_Q(A)$ of degree $n$ is a linear combination of terms that look like*

$$q_1 \cdot \ldots \cdot q_n + Q^{n+1} = (q_1 + Q^2) \cdot \ldots \cdot (q_n + Q^2).$$

○

Now take a stable $Q$-filtration $(M_n)$ of $M$, where $M_0 = M$, and define

$$G_Q(M) = \bigoplus_n M_n/M_{n+1} = \bigoplus_n M_n/QM_n.$$

$G_Q(M)$ is a $G_Q(A)$-module *e.g. multiplication works like*

$$(q^2 + Q^3)(m_n + QM_n) = q^2 m_n + Q^3 M_n \in M_{n+2}/M_{n+3}.$$

which is finitely-generated because $M$ is finitely-generated over $A$. Define $s$ to be the minimal number of generators of $Q$. This is equal to $\dim_k(Q/\mathfrak{m}Q)$ by Corollary 2.10.

Now we can apply the previous theorems.

PROPOSITION 10.5. *(9.4) Let $(A, \mathfrak{m}, k)$ be a local Noetherian ring, $M$ a finitely-generated $A$-module, and $Q$ an $\mathfrak{m}$-primary ideal. Let $(M_n)$ be a stable $Q$-filtration.*

(1) *$M/M_n$ has finite length.*
(2) *There is a polynomial $g(t) \in \mathbb{Q}[t]$ with $\deg g \leq s$ where $Q$ is generated over $A$ by $s$ elements*, such that $\ell(M/M_n) = g(n)$ for $n$ sufficiently large.
(3) The degree and leading coefficient of $g$ are independent of filtration chosen.

*Proof.* *(1) We have a filtration $M = M_0 \supset M_1 \supset M_2 \supset \cdots$. Consider the series*

$$M = M/M_n \supset M_1/M_n \supset \cdots \supset M_n/M_n = 0$$

*By Corollary 6.4, it suffices to show that the quotients*

$$(M_i/M_n)\Big/(M_{i+1}/M_n) \cong M_i/M_{i+1}$$

*have finite length. Since they are $A/Q$-modules (check that $Q$ annihilates $M_i/M_{i+1}$), it suffices to show that they have finite length over $A/Q$.*

CLAIM. $A/Q$ is both Noetherian and Artinian.

*Proof of claim.* $A$ is Noetherian so $A/Q$ is Noetherian. We showed $A/Q$ is Artinian in Claim 10.3. ○

CLAIM. $M_i/M_{i+1}$ is both Noetherian and Artinian.

*Proof of claim.*

$$\begin{aligned} M \text{ Noetherian} &\implies M_i \text{ is finitely generated over } A \\ &\implies M_i \text{ is Noetherian} \\ &\implies M_i/M_{n+1} \text{ is Noetherian} \\ &\implies M_i/M_{n+1} \text{ is finitely-generated over } A \\ &\implies M_i/M_{n+1} \text{ is finitely-generated over } A/Q \end{aligned}$$

Since $A/Q$ is Artinian and Noetherian, $M_i/M_{n+1}$ is too. ○

CLAIM. $M_i/M_{n+1}$ has finite length.

*Proof of claim.* Proposition 6.8 in Atiyah/ Macdonald (Noetherian + Artinian $\iff$ finite length.) ○

(2) Pick generators $x_1, \cdots, x_s$ of $Q$. Write $\overline{x}_i = x_i \pmod{Q^2}$. So the $\overline{x}_i$'s generate $G_Q(A)$ as an $A_0$-algebra. By Corollary 9.2, $\ell(M_n/M_{n+1}) = f(n)$ for some $f \in \mathbb{Q}[t]$, for sufficiently large $n$, and $\deg f \leq s - 1$.

So $\ell(M/M_{n+1}) - \ell(M/M_n) = f(n)$. *Use Lemma 6.8(3) (additivity of length over short exact sequences) and the following:*

$$0 \to M_n \to M \to M/M_n \to 0$$

$$0 \to M_{n+1} \to M \to M/M_{n+1} \to 0$$

*which give* $\ell(M) = \ell(M/M_n) + \ell(M_n) = \ell(M/M_{n+1}) + \ell(M_{n+1})$ *so it suffices to prove* $\ell(M_n/M_{n+1}) = \ell(M_n) - \ell(M_{n+1})$ *which comes from doing the same thing to*

$$0 \to M_{n+1} \to M_n \to M_n/M_{n+1} \to 0.$$

$$\ell(M/M_{n+1}) = \ell(M/M_{n+1}) - \underbrace{\ell(M/M_0)}_{=\ell(M/M)=0}$$

$$= \sum_0^n f(n) = \int_0^{n+1} f(x)\ dx$$

which is a polynomial $g(n)$ of degree $\leq s$.

(3) Suppose $(\widetilde{M_n})$ is another stable filtration with $\ell(M/\widetilde{M_n}) = \widetilde{g}(n)$ for large enough $n$. By Lemma 8.4, there is some $n_0$ such that

$$M_{n+n_0} \subset \widetilde{M_n}$$

and

$$\widetilde{M}_{n+n_0} \subset M_n$$

for all $n$. So $\widetilde{g}(n+n_0) \geq g(n)$, and $g(n+n_0) \geq \widetilde{g}(n)$. So

$$\lim_{n\to\infty} \frac{\widetilde{g}(n)}{g(n)} = 1.$$

○

If $M_n = Q^n M$ then let $\chi_Q^M := g$. So $\chi_Q^M(n) = \ell(M/Q^n M)$ for large enough $n$. Write $\chi_Q := \chi_Q^A$.

Corollary 10.6. *(9.5) There exists a polynomial* $\chi_Q$ *of degree* $\leq s$ *such that* $\ell(A/Q^n) = \chi_Q(n)$ *for all* $n$ *large enough (where* $s$ *is the minimal number of generators of* $Q$*).*

Proposition 10.7. *(9.6)*

$$\deg\ \chi_Q = \deg\ \chi_{\mathfrak{m}}$$

*(If I take a different primary ideal, I will get a different polynomial, but the degree will be the same.)*

*Proof.* $\mathfrak{m} \supset Q \supset \mathfrak{m}^r$, so $\mathfrak{m}^n \supset Q^n \supset \mathfrak{m}^{rn}$. So $\chi_{\mathfrak{m}}(n) \leq \chi_Q(n) \leq \chi_{\mathfrak{m}}(rn)$. Since $\chi_{\mathfrak{m}}$ and $\chi_Q$ are polynomials, the result follows. (This gives $\deg\ \chi_{\mathfrak{m}}(n) \leq \deg\ \chi_Q(n) \leq \deg\ \chi_{\mathfrak{m}}(rn)$. If the first inequality is strict, then you will eventually break the second inequality.) ○

Let $d(A) := \deg\ \chi_Q$, which is independent of $Q$. $d(A)$ measures the order of growth of $\ell(A/Q^n)$. Define

$$\delta(A) = \min_{\substack{\mathfrak{m}\text{-primary} \\ Q}} \{\dim_k(Q/\mathfrak{m}Q)\}$$

This is the least number of generators of any $\mathfrak{m}$-primary ideal.

Let $\dim(A)$ be the maximum length of any chain of prime ideals in $A$, where "length of chain" means that

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

has length $r$. We shall see that $\delta(A) \geq d(A) \geq \dim(A) \geq \delta(A)$, and so **they are all equal**.

Proposition 10.8. *(9.7)*

$$\delta(A) \geq d(A)$$

*Proof.* Already done this: 9.5 and 9.6. ○

Proposition 10.9. *(9.8) Assume $x \in M$ is not a zero-divisor in $M$. Take $M' = M/xM$. Then*

$$\deg\ \chi_Q^{M'} \leq \deg\ \chi_Q^M - 1.$$

*Proof.* Let $N = xM$, and $M' = M/N$. $x$ is not a zero-divisor in $M$, so $N \cong M$. Define $N_n = N \cap (Q^n M)$, which is a stable $Q$-filtration of $N$ by the Artin-Rees Lemma. There is an exact sequence

$$0 \to N/N_n \to M/Q^n M \to M'/Q^n M' \to 0$$

Define $g(n) := \ell(N/N_n)$. Then $g(n) - \chi_Q^M(n) + \chi_Q^{M'}(n) = 0$ for $n$ large.

Then by 9.4, $g(n)$ and $\chi_Q^M$ have the same leading term ($g(n)$ corresponds to $N$ and $\chi_Q^M$ corresponds to $M$, but $N \cong M$). *So $\chi_Q^{M'}(n) = \chi_Q^M(n) - g(n)$ has degree strictly smaller than $\chi_Q^M(n)$ because the leading term is knocked out.* ○

## Saturday optional lecture – October 27

Start with a plane $X$ (or $\mathbb{P}^1$) with (homogeneous) coordinages $x_1, x_2$. Over the field $k$, in order to change coordinates we're forced to deal with the group $GL_{2,k}$ of linear transformations. (In the projective case, this is $PGL_2$.) Consider $G = SL_{2,k}$, a three-dimensional object (4 coordinates, 1 relation). $G$ acts on $X$; then $G$ acts on the ring $k[V]$ of polynomial functions on $V$. If $\varphi$ is a function, then $g(\varphi)(g(v)) = \varphi(v)$. $X^* =$ {linear functions} and $Sym^n(X^*) =: V(n)$ are the homogeneous functions of degree $n$. Then $\dim V(n) = n+1$ because there's a basis $x_1^n, x_1^{n-1}x_2, \cdots, x_2^n$. This is a representation of $G = SL_2$.

The map $SL_2 = G \xrightarrow{\pi_n} GL(V(n))$ is a homomorphism of groups, and is a morphism of affine algebraic varieties. A representation of a group $G$ differentiates to give a representation of $Lie(G) := T_eG$ (tangent space at the origin). Let $X \in Lie(G)$. Then $X = \lim_{t\to 0} g(t)$, where $g(0) = e$. $X$ acts on $v$ by $X(v) = \lim_{t\to 0} \frac{g(t)(v)-v}{t}$. $V(n)$ is a representation of $Lie(SL_2)$, which is semisimple: every finite-dimensional representation of a semisimple in characteristic zero is completely reducible. Then $\{V(n)\}$ is a complete list of the finite-dimensional irreducible reps. of $Lie(SL_2)$.

Every representation of the group can be differentiated to get a representation of the Lie algebra. But this doesn't work in reverse when the representation is infinite-dimensional.

If $V, W$ are finite-dimensional vector spaces, then $V \otimes_k W$ is also a representation of $G$: $g(v \otimes w) = g(v) \otimes g(w)$. Differentiation works by

$$X(v \otimes w) = X(v) \otimes w + v \otimes X(w)$$

for $g \in G$, $X \in Lie(G)$. A representation of the group that is irreducible as a representation of the algebra, is also irreducible as a representation f the group: just take a possible ideal and differentiate.

Theorem (Clebsch-Gordan Rule).

$$V(m) \otimes V(n) \cong V(m+n) \oplus V(m+n-2) \oplus \cdots \oplus V(|m-n|)$$

Also, $Sym^r V(m)$ is a representation of $G$. It has a decomposition: i.e. there are $G$-equivariant linear maps $Sum^r V(m) \to V(p)$ for various $p$. This is the same as a $G$-equivariant polynomial map $V(m) \to V(p)$; these are called *covariants*. An *invariant* is a covariant for $V(p) = V(0) = k$ with the trivial $G$-action.

For example, $V(2)$ is the space of binary quadratic forms in 2 variables; the discriminant is an invariant:

$$\Delta(ax_1^2 + 2bx_1x_2 + cx_2^2) = ac - b^2.$$

Another example is the cross-ratio of 4-points, which tells whether one can move between such 4-tuples using linear transformations.

So, what are the invariants for $V(n)$? An $n$-homogeneous polynomial corresponds to $n$ linear factors, each of which corresponds to a point in projective space. So these are equivalent to unordered collections of $n$ points in $\mathbb{P}^1$. We want invariants because they tell which collections of points are equivalent. $k[V_n]^{SL_2}$ is the ring of invariants; $k[V_n]$ is a polynomial ring in $n+1$ variables. We seek an inclusion $k[V_n]^{SL_2} \hookrightarrow k[V_n]$.

Let's construct invariants. Let $f(\mathbf{x}) = f(x_1, x_2) \in V(n)$. Then

$$f = \sum_{i=0}^{n} \binom{n}{i} A_i x_1^{n-i} x_2^i$$

We're looking for collections of $A_i$'s that are invariant. Write

$$a_x = a_1x_1 + a_2x_2$$

$$b_x = b_1x_1 + b_2x_2$$
$$\cdots$$

Write $(ab) = a_1b_2 - a_2b_1$. Pretend that $f = a_x^n = b_x^n = \cdots$; then $(ab)^n$ is an invariant. For example, if $n = 4$, then $(ab)^4$ is an invariant, as is $(ab)^2(ac)^2(bc)^2$. The $a, b, c$ are distinct, subject to relations

$$a_1^{n-i}a^i = A_i$$
$$b_1^{n-i}b^i = A_i$$

So

$$\begin{aligned}(ab)^4 = (a_1b_2 - a_2b_1)^4 &= a_1^4b_2^4 - 4a_1^3a_2b_1b_2^3 + 6a_1^2a_2^2b_1^2b_2^2 - 4 - 4a_1a_2^3b_1^3b_2 + a_2^4b_1^4\\ &A_0A_4 - 4A_1A_3 + 6A_2^2 - 4A_3A_1 + A_4A_0\\ &= 2(A_0A_4 - 4A_1A_3 + 3A_2^2)\end{aligned}$$

is an invariant of $V(4)$. $SL_2$ is defined by the property that it leaves $(ab)$ invariant, so $(ab)^4$ is invariant.

$$f(x) = f(x_1, x_2) = \left(x_1\frac{\partial}{\partial y_1} + x_2\frac{\partial}{\partial y_2}\right)^n (\frac{1}{n!}f(y_1, y_2)) = \left(x_1\frac{\partial}{\partial z_1} + x_2\frac{\partial}{\partial z_2}\right)^n (\frac{1}{n!}f(z_1, y_2))$$

This is $b_x^n(\frac{1}{n!}f(z_1, z_2))$ if $b_j = \frac{\partial}{\partial z_j}$. I claim

$$\begin{aligned}(ab)^r a_x^{n-r}b_x^{n-r} = &\left(\frac{\partial}{\partial y_1}\frac{\partial}{\partial z_2} - \frac{\partial}{\partial y_2}\frac{\partial}{\partial z_2}\right)^r \left(x_1\frac{\partial}{\partial y_1} + x_2\frac{d}{\partial y_2}\right)^{n-r} \cdot\\ &\left(x_1\frac{\partial}{\partial z_1} + x_2\frac{\partial}{\partial z_2}\right)^{n-r} \cdot \left(\frac{1}{n!^2}\cdot f(y_1, y_2)\cdot f(z_1, z_2)\right)\end{aligned}$$

The previous theorem works by sending

$$a_x^m \otimes \alpha_x^n \mapsto \left(a_x^m \cdot \alpha_x^n, (a\alpha)a_x^{m-1}\cdot\alpha_x^{n-1}, (a\alpha)^2a_x^{m-2}\alpha_x^{n-2}, \cdots, (a;a)^d a_x^{n-d}\right)$$

if $m \le n$ and $d = n - m$.

THEOREM 10.1 (Hilbert). *Suppose $G$ is any semisimple algebraic group, $V$ a representation of $G$, over a field $k$ of characteristic 0. Then the subring of invariants $k[V]^G$ is finitely generated.*

DEFINITION 10.2. Suppose $G$ acts on $V$. $v \in V$ is *stable* if its orbit $G(v) \subset V$ is Zariski-closed, and $Stab(v)$ is finite.

Suppose $v_1, v_2 \in V$, and $v_1$ is stable. Then $v_1 \overset{G}{\sim} v_2$ iff all invariants are equal.

On $\mathbb{P}^1$, there are three possibilities: three distinct points, two points that are equal, and all three points are equal. These are different, but cannot be distinguished by invariants. $v$ is stable if, whenever you choose a basis $\{e_\alpha\}$ of $V$ that consists of eigenvectors for a

1-parameter subgroup of $G$ (isomorphic to a 1-dimensional torus) then when you write

$$v = \sum \lambda_\alpha e_\alpha$$

with $\lambda_\alpha \neq 0$, both $> 0$ and $< 0$ weights appear. For example, a maximal torus in $SL_2$ is $\begin{pmatrix} t & 0 \\ 0 & -t \end{pmatrix}$, and $x_1^2 x_2$ (the situation with two doubled points and a third distinct) has weight 1.

# Lecture 11: October 29

Let $(A, \mathfrak{m}, k)$ be a Local Noetherian ring. Then we were discussing three quantities:

- $d(A)$ was the degree of the polynomial $\ell(A/\mathfrak{m}^n)$ (i.e. there exists a polynomial in one variable $n$ which, for sufficiently large values of $n$, agrees with this length).
- $\delta(A)$ was the minimum number of generators of an $\mathfrak{m}$-primary ideal.
- $\dim A$ is the maximum length of a chain of prime ideals in $A$.

Suppose $A$ was the local ring of a point $P$ in an algebraic variety $V$ over $k$. $d(A)$ is more purely algebraic; we are more interested in showing $\delta(A) = \dim A$, and will do so by showing they are both equal to $d(A)$. The other two have more geometric meanings: $\delta(A)$ is the minimum number of hypersurfaces (i.e. varieties defined by one function) passing through $P$ that are required to cut $V$ down to $P$. $\dim(A)$ is the maximal length of a chain of subvarieties of $V$ through $P$. Also, $\dim(A) = \dim(v) := tr[k(v) : k]$, where $v$ is a variety, and transcendence degree is the maximum number of elements in $k(v)$ that are algebraically independent over $k$. The idea is that the functions defining the hypersurfaces give a transcendence basis, and this measures the number of independent functions (or, degrees of freedom in which a point can move).

Our aim is to prove

$$\delta(A) \geq d(A) \geq \dim(A) \geq \delta(A)$$

and we've done the first inequality.

Last time, we had an $\mathfrak{m}$-primary ideal $Q$. If $M$ is a finitely-generated $A$-module, then $\ell(M/Q^n M) = \chi_Q^M(n)$ is a polynomial in $n$ (where the equality works for $n \gg 0$).

Proposition 11.1. *If $x \in \mathfrak{m}$ is not a divisor in $M$, and $M' = M/xM$, then* $\deg \chi_Q^{M'} \leq \deg \chi_Q^M - 1$.

Corollary 11.2. *(9.9) If $x$ is a non-zero-divisor in $A$, then $d(A/(x)) \leq d(A) - 1$.*

Proposition 11.3. *(9.10)*

$$d(A) \geq \dim(A)$$

*(We're not assuming that* $\dim(A)$ *is finite, in order to prove this.)*

*Proof.* Induction on $d(A)$. If $d(A) = 0$, then $\ell(A/\mathfrak{m}^n)$ is constant for $n$ sufficiently large. So $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some $n$. Read this as $\mathfrak{m} \cdot (\mathfrak{m}^n) = \mathfrak{m}^n$. By Nakayama's lemma, $\mathfrak{m}^n = 0$. Then $A$ is Artinian *by 6.10*, so $\mathfrak{m}$ is the only prime ideal, and so $\dim A = 0$.

Assume $d(A) > 0$, and suppose I have a chain of prime ideals

$$P_0 \subsetneq \cdots \subsetneq P_r.$$

I need to show that $r \leq d(A)$. Choose $x \in P_1 - P_0$, and put $A' = A/P_0$. Set $x'$ to be the image of $x$ in $A'$, which is nonzero. Since $A/P_0$ is an integral domain, we can invoke Corollary 9.9 which shows $d(A'/(x')) \leq d(A') - 1$.

*Let $\mathfrak{m}'$ be the maximal ideal of $A'$.* Since $A \twoheadrightarrow A'$ is a surjection, $A/\mathfrak{m}^n \twoheadrightarrow A'/\mathfrak{m}'^n$ is a surjection. So $d(A/\mathfrak{m}^n) \geq d(A'/\mathfrak{m}'^n)$, which in turn shows that $d(A) \geq d(A')$. So

$$d(A'/(x')) \leq d(A') - 1 \leq d(A) - 1.$$

The length of any chain of prime ideals in $A'/(x')$ is $\leq d(A') - 1$ (by induction). In $A'/(x')$ we have the chain

$$P_1/(P_0 + (x)) \subsetneq P_2/(P_0 + (x)) \subset \cdots \subset P_r/(P_0 + (x))$$

which has length $r - 1$. So $r - 1 \leq d(A') - 1 \leq d(A) - 1$. ○

Corollary 11.4. *(9.11)* $\dim(A)$ *is finite.*

Definition 11.5. If $A$ is any Noetherian ring, and $P$ is a prime ideal, we can define the *height* of $P$ by

$$ht(P) = \dim(A_P) = \begin{array}{c}\text{maximal length of an ascending chain} \\ \text{of prime ideals terminating at } P\end{array}$$

Definition 11.6. A *minimal prime ideal* $P$ of an ideal $I$ is one that is minimal among all primes containing $I$. (That is, if $P' \subset P$ is a prime containing $I$ then $P' = P$.)

Equivalently, the minimal primes of $I$ are the primes $P_i$ appearing in the unique irredundant expression $\sqrt{I} = \bigcap P_i$.

Proposition 11.7. *(9.13) Suppose that* $\dim A = d$ *(and $A$ is local). Then there exists an $\mathfrak{m}$-primary ideal $Q$ generated by $d$ elements $x_1, \cdots, x_d$. Therefore,* $\dim A \geq \delta(A)$.

*Proof.* Construct $x_1, \cdots, x_i$ (for $i \leq d$) inductively, with the property that every prime ideal containing $(x_1, \cdots, x_i)$ has height $\geq i$. Suppose $i > 0$ and $x_1, \cdots, x_{i-1}$ have been constructed. Say $\{P_j : 1 \leq j \leq s\}$ are the minimal prime ideals of $(x_1, \cdots, x_{i-1})$ whose height is exactly $i - 1$ (there might be none of them). Since $i - 1 < d = ht(\mathfrak{m})$, $P_j \neq \mathfrak{m}$, and therefore $\mathfrak{m} \neq \bigcup_{j=1}^s P_j$. Choose $x_i \in \mathfrak{m} - \bigcup_1^s P_j$.

Let $Q$ be some prime containing $(x_1, \cdots, x_i)$. So $Q$ contains some minimal prime $P$ of $(x_1, \cdots, x_{i-1})$. If $P$ is some $P_i$, then $x_i \in Q$, $x_i \notin P$, so $Q \supsetneq P$, so $ht(Q) \geq i$. If $P \neq$ any $P_j$, then $ht(P) \geq i$, so $ht(Q) \geq i$. So every prime ideal containing $(x_1, \cdots, x_i)$ has height $\geq i$.

If $i = d$, then every prime ideal $Q$ containing $(x_1, \cdots, x_d)$ has height $d$, and so $Q = \mathfrak{m}$. In other words, $A' := A/(x_1, \cdots, x_d)$ has only one prime ideal. so is Artinian, so $nil(A') = \mathfrak{m}/(x_1, \cdots, x_d)$; i.e. $(x_1, \cdots, x_d)$ is $\mathfrak{m}$-primary. ○

COROLLARY 11.8 (The dimension theorem). *(9.14)*

$$d(A) = \dim(A) = \delta(A)$$

EXAMPLE 11.9. $A = k[X_1, \cdots, X_d]_{(X_1, \cdots, X_d)}$ has $\dim A = d$, because the associated graded ring $G_{\mathfrak{m}}(A) \cong k[x_1, \cdots, x_d]$, where $x_i = X_i$ modulo $\mathfrak{m}^2$. The Poincaré series for this ring is $\frac{1}{(1-t)^d}$.

COROLLARY 11.10. *(9.15)*

$$\dim A \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$$

*Proof.* Nakayama's lemma says: for any finitely-generated $A$-module $M$, $\dim_k(M/\mathfrak{m}M) =$ the minimal number of generators of $M$. Take $M = \mathfrak{m}$. Use $\dim(A) = \delta(A)$ to get the result. ○

DEFINITION 11.11. $A$ is *regular* if $\dim A = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

For varieties $V$ defined over perfect fields, and $P \in V$ a $k$-point, the local ring $\mathcal{O}_{V,P}$ is regular iff the variety is smooth at that point.

Get a basis of the cotangent space $\mathfrak{m}/\mathfrak{m}^2$ – this is a collection of differential objects $df$. These allow you to locally embed your variety into affine space.

# LECTURE 12: OCTOBER 31

RECALL we had a local ring $(A, \mathfrak{m}, k)$ and were discussing

- $d(A)$, which measures the rate of growth of $\ell(A/\mathfrak{m}^n)$
- $\delta(A)$, the minimum number of generators of an $\mathfrak{m}$-primary ideal
- $\dim(A)$ (the Krull dimension), the maximal length of a chain of prime ideals in $A$.

Last time, we proved these were all equal.

COROLLARY 12.1. *(9.16) Suppose $x_1, \cdots, x_r \in \mathfrak{m}$. Then every minimal prime $p$ containing all $x_i$ has height $\leq r$.*

*Proof.* In $A_p$, the ideal $(x_1, \cdots, x_r)$ is $p_p$-primary, by minimality. Then $r \geq \delta(A_p) = \dim(A_p) =: ht(p)$. ○

REMARK 12.2 (Krull's principal ideal theorem). If $x \in \mathfrak{m}$ and $x$ is not a zero-divisor, and $p$ is minimal containing $x$, then $ht(p) = 1$.

For example, if $V$ is an algebraic variety over $k$, and $p \in V$ is a closed point, and $A = \mathcal{O}_{V,p}$, then $\text{im}(A) = \dim(V) := tr.deg.[k(V) : k]$. (This will be on the example sheet.)

Why can't you have two chains $p \to \cdots \to q$ of different lengths? This *can* happen in an arbitrary Noetherian ring, but it can't happen in the rings you care about in algebraic geometry; in particular, it doesn't happen in Cohen-Macaulay rings. This includes regular rings (such as fields and Dedekind domains), and $A[x]$ if $A$ is Cohen-Macaulay. $A$ is regular if $A_{\mathfrak{m}}$ is regular for all maximal $\mathfrak{m}$. You can show that this is equivalent to $A_p$ being regular for all primes $p$.

**Tensor products and flatness.** Start with a ring $A$ (not necessarily Noetherian), with $M, N$ two $A$-modules. We want to construct $M \otimes_A N$, an $A$-module, the tensor product of $M, N$ over $A$. If $\{m_\alpha\}_{\alpha \in I}$ is a generating set of $M$, and if $\{n_\beta\}_{\beta \in J}$ is a generating set for $N$, then the symbols $\{m_\alpha \otimes n_\beta\}_{(\alpha,\beta) \in I \times J}$ should generate the module $M \otimes_A N$. But I don't want to construct it as the linear combinations of $m_\alpha \otimes n_\beta$, because that will be basis-dependent.

For example, suppose $A = k$ is a field, and $M$ and $N$ are finite-dimensional vector spaces over $k$ that are representations of a group $G$. Then $M \otimes_A N$ will also be a representation of $G$, and $g(m \otimes n) = g(m) \otimes g(n)$.

We also want $\dim(M \otimes N) = \dim(M) \cdot \dim(N)$.

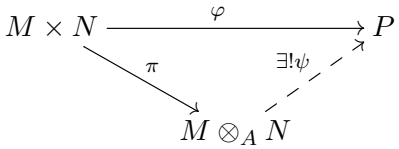
If $M$ and $N$ are free modules, $M \otimes N$ should be a free module of rank $rk(M) \cdot rk(N)$.

We construct $M \otimes N$ as a solution to a universal mapping property. Fix $M, N$. If $P$ is a third $A$-module, then an $A$-bilinear map $\varphi : M \times N \to P$ is a map such that

$$\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n) \ \forall m_1, m_2, n \in M$$
$$\varphi(am, n) = a \cdot \varphi(m, n) \ \forall n \in N, a \in A$$

and similarly in the second argument.

PROPOSITION 12.3. *Given $M, N$, there is an $A$-module $M \otimes_A N$ and a bilinear map $\pi : M \times N \to M \otimes_A N$ such that for every bilinear map $\varphi : M \times N \to P$, there is a unique factorisation of $\varphi$ through $\pi$:*




*Proof.* Any module $X$ has a canonical (but hugely inefficient) set of generators, namely $X$. That is, $X$ is canonically a quotient of the free module $F = A^X$ (the free module on the set $\{e_x : x \in X\}$). Then there s a canonical surjection

$$F \overset{\pi}{\twoheadrightarrow} M \text{ where } \pi(\sum_{finite} a_x e_x) = \sum a_x x$$

Define $C = A^{M\times N}$; any element of $C$ is of the form

$$\sum_{(m,n)\in M\times N} a_{(m,n)}e_{(m,n)}$$

Define $D \subset C$ to be the submodule generated by the following kinds of elements:

(1) $e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}$
(2) $e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}$
(3) $e_{am,n} - a \cdot e_{(m,n)}$
(4) $e_{(m,a_n)} - a \cdot e_{(m,n)}$

for all $m, m' \in M$, $n, n' \in N$, $a \in A$.

Define $T := C/D$. There is a bilinear map $\pi : M \times N \to T$ given by $\pi(m,n) = e_{(m,n)} \pmod D$; this is bilinear exactly because we've modded out by $D$: we need $\pi(am,n) = a\cdot\pi(m,n)$; therefore we need $e_{(am,n)} = a\cdot e_{(m,n)}$, which is that was forced on us by modding out by $D$.

Now I have to show that $T$ satisfies the conditions in the proposition. Given any bilinear map $\varphi : M \times N \to P$, there is a homomorphism

$$\Psi : C \to P \text{ where } \Psi(e_{(m,n)}) = \varphi(m,n)$$

The bilinearity of $\varphi$ forces $\Psi$ to kill $D$, so we get a map $\psi : T \to P$, where $\psi(e_{(m,n)} \pmod D) = \varphi(m,n)$. Check that $\psi \circ \pi = \varphi$.

So we define $T =: M \otimes_A N$. ○

When you construct something as a solution to a universal mapping property, then any two solutions are isomorphic up to unique isomorphism. So $M \otimes_A N$ is well-defined.

Lemma 12.4. *(10.3) Given modules $M, N, P$, there is a canonical isomorphism*

$$\mathrm{Hom}_A(M \otimes_A N, P) \to \mathrm{Hom}_A(M, \mathrm{Hom}(N,P)).$$

*Proof.* There is a canonical isomorphism

$$\mathrm{Hom}_A(M \otimes_A N, P) = Bilin(M \times N, P)$$

Then there is a map

$$Bilin(M \times N, P) \xrightarrow{\alpha} \mathrm{Hom}(M, \mathrm{Hom}(N,P))$$

sending $\varphi \mapsto \varphi'$ where $(\varphi'(m))(n) = \varphi(m,n)$. It is easy to see that $\alpha$ is an isomorphism. ○

Definition 12.5. A sequence

$$\cdots \to M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} \cdots$$

is a *chain complex* if every $f_i \circ f_{i+1} = 0$; in other words, you need $\mathrm{im}(f_{i+1}) \subset \ker(f_i)$.

Given $M, P, Q$ and a homomorphism $P \stackrel{g}{\to} Q$, there is an induced homomorphism $M \otimes P \stackrel{Id_M \otimes g}{\to} M \otimes Q$. Why? To construct $Id_M \otimes g$, it's enough to construct $\mathrm{Hom}(M \otimes P, Y) \leftarrow \mathrm{Hom}(M \otimes Q, Y)$ for all modules $Y$. That is, we must construct $Bilin(M \times P, Y) \leftarrow Bilin(M \times Q, Y)$ for all $Y$. Do this by sending $\varphi : M \times Q \to Y$ to $\varphi' : M \times P \to Y$ that is defined by $\varphi'(m, p) = \varphi(m, g(p))$.

# Lecture 13: November 2

Last time we talked about tensor products. Suppose $A$ is a ring, and $M, N, P, \cdots, X, Y$ are $A$-modules. We constructed $M \otimes_A N$ as a quotient: it comes with a bilinear map $M \times N \stackrel{\pi}{\to} M \otimes_A N$ where $\pi(m, n) = m \otimes n$, and $Bilin(M \times N, P) = \mathrm{Hom}(M \otimes_A N, P)$ for all $P$.

For example,

$$(m + m') \otimes n = m \otimes n + m' \otimes n$$

and

$$(am) \otimes n = a(m \otimes n) = m \otimes (an).$$

Every element of $M \otimes N$ is a linear combination $\sum a_i(m_i \otimes n_i)$.

Lemma 13.1. *A homomorphism $g : X \to Y$ induces a homomorphism $M \otimes_A X \stackrel{1_M \otimes g}{\to} M \otimes_A Y$, where $(1_M \otimes g)(M \otimes x) = m \otimes g(x)$.*

*Proof.* To construct this, we need a bilinear map $M \times X \to M \otimes_A Y$; just take $(m, x) \mapsto m \otimes g(x)$. You show that it's an isomorphism. ○

We have a natural map $A \otimes_A M \stackrel{\cong}{\to} M$ that arises from the bilinear map $A \times M \to M$ given by $(a, m) \mapsto am$. So send $a \otimes m \mapsto am$. To show this is an isomorphism, show that whenever I compose this with a map to a module $P$, that is an isomorphism.

There is also an isomorphism $M \otimes_A N \stackrel{\cong}{\to} N \otimes_A M$, arising from the bilinear map $M \times N \to N \otimes_A M$ given by $(m, n) \mapsto n \otimes m$. So we send $m \otimes n \mapsto n \otimes m$. But $m \otimes m'$ is not the same element in $M \otimes M$ as $m' \otimes m$. Moral: the tensor product is not commutative at the level of elements.

$$(M \otimes_A N) \otimes_A P \stackrel{\cong}{\to} M \otimes_A (N \otimes_A P)$$

because both sides are isomorphic to the module $M \otimes_A N \otimes_A P$ constructed from solving a universal mapping property involving trilinear maps.

The tensor product is also distributive:

$$M \otimes_A \left( \bigoplus_\alpha N_\alpha \right) \stackrel{\cong}{\to} \bigoplus_\alpha (M \otimes_A N_\alpha)$$

is given by the map $m \otimes (n1, \cdots, n_r) \mapsto (m \otimes n_1, \cdots, m \otimes n_r)$. (We're leaving out the step with the bilinear map, but you get the idea.) In particular, $M \otimes A^m \cong M^{\oplus m}$.

Also a commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & Z \end{array}$$

gives a commutative diagram

$$\begin{array}{ccc} M \otimes X & \longrightarrow & M \otimes Y \\ & \searrow & \downarrow \\ & & M \otimes Z \end{array}$$

Given a chain complex

$$M_* = \cdots \to M_{i+1} t \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} \cdots$$

we get a complex

$$M_* \otimes N = \cdots \to M_{i+1} \otimes N \xrightarrow{f_{i+1} \otimes 1_N} M_i \otimes N \to \cdots$$

By the functorial nature of taking the tensor product, if $f_i \circ f_{i+1} = 0$, then $(f_i \otimes 1_N) \circ (f_{i+1} \otimes 1_N) = 0$ as well, so we really get a chain complex out of this.

Lemma 13.2. *(10.6)*

(1) *A sequence*
$$M' \to M \to M'' \to 0$$
*is exact iff, for all modules $P$, the sequence*
$$0 \to \mathrm{Hom}(M'', P) \to \mathrm{Hom}(M, P) \to \mathrm{Hom}(M', P)$$
*is exact.*

(2) *A sequence*
$$0 \to M' \to M \to M''$$
*is exact iff, for all $P$,*
$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$$
*is exact.*

*Proof.* Trivial. Do note that this is false when you look at longer exact sequences (i.e. if you try putting a zero before $M'$ in (1), it's not going to work). Also note the reversal of the arrows in (1). ○

Proposition 13.3. *(10.7) If*
$$M' \to M \to M'' \to 0$$
*is exact, then so is*
$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
*(where $\otimes$ means $\otimes_A$).*

*Proof.* By the previous lemma, we need

$$0 \to \mathrm{Hom}(M'' \otimes N, P) \to \mathrm{Hom}(M \otimes N, P) \to \mathrm{Hom}(M' \otimes N, P)$$

to be exact, for all $P$. Convert this into bilinear maps: we want

$$0 \to Bilin(M'' \times N, P) \to Bilin(M \times N, P) \to Bilin(M' \times N, P)$$

to be exact for all $P$.

Exercise: finish this. ○

This is summarised by saying *the tensor product is right exact.*

Definition 13.4. $N$ is *flat* if, for every short exact sequence

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

the sequence

$$0 \to N \otimes M' \to N \otimes M \to N \otimes M'' \to 0$$

is exact. (It does not matter if you take the $\otimes$ on the right or left; "right" in right exact refers to the sequence, not the side the tensor product is taken on.)

Lemma 13.5. *(10.9) Suppose that $N$ is a finitely-presented $A$-module (not necessarily Noetherian). Then TFAE:*

1. *$N$ is flat;*
2. *$N_P$ is flat as an $A_P$-module for all primes $P$;*
3. *$N_{\mathfrak{m}}$ is flat as an $A_{\mathfrak{m}}$-module for all maximal $\mathfrak{m}$;*
4. *$N_P$ is a free $A_P$-module for all primes $P$;*
5. *$N_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module for all maximal $\mathfrak{m}$;*
6. *$N$ is a direct summand of a finite free $A$-module;*
7. *there exists $s_1, \cdots, s_r \in A$ such that $(s_1, \cdots, s_r) = A$ and for every $i$, $S_i^{-1}N$ is a free $S_i^{-1}A$-module, where $S_i = \{s_i^n : n \geq 0\}$. Even if $A$ is not Noetherian, you can always reduce an infinite generating set of $A$ over $A$ to a finite one, just by noticing that $1$ is generated by finitely many things.*

Remark 13.6. This does not work in general for rings that are just finitely generated, not finitely presented. Recall that $M$ is finitely presented if it has finitely many generators and finitely many relations; that is, if there is an exact sequence $F_1 \to F_0 \to M \to 0$ where $F_0$ and $F_1$ are both free and of finite rank. (The basis elements of $F_1$ map to the *relations* needed to get $M$ from $F_0$.)

Remark 13.7. Modules satisfying the property in (7) are called *locally free*. For example, if $A = k[V]$ (where $V$ is a variety over $k$), then $S_i^{-1}A = A[s_i^{-1}] = k[V - (s_i = 0)]$. (If your ring is a ring of functions, inverting a function is the same as deleting the locus where it's zero.) Say $U_i = V - (s_i = 0)$. If the $s_i$'s fail to generate, then $(s_1, \cdots, s_r)$ is contained in some maximal ideal; by the Nullstellensatz that corresponds to a point that is excluded by all $U_i$. That is, $V = \bigcup U_i$ precisely because $(s_1, \cdots, s_r) = A$.

Now suppose we have an $A$-algebra $C$ and a homomorphism $g : A \to C$, and an $A$-module $M$. (In particular, $C$ is an $A$-module.)

LEMMA 13.8. *$M \otimes_A C$ is naturally a $C$-module, and it is universal w.r.t. $A$-module homomorphisms $M \xrightarrow{\varphi} Q$, where $Q$ is a $C$-module: define $\psi : M \otimes_A C \to Q$ by $\psi(m \otimes c) = c \cdot \varphi(m)$.*

*Suppose $M$ is given in terms of generators and relations. There is an exact sequence*

$$F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

*where $F_0$ is the free module on the generators of $M$. This has a kernel $K$, which is finitely generated, so we can construct $F_1 \to K \hookrightarrow F_0$ in the same way. This produces the sequence above. You could keep going with this but we won't now.*

*Now*

$$F_1 \otimes_A C \xrightarrow{\varphi_1 \otimes 1_C} F_0 \otimes C \xrightarrow{\varphi_0 \otimes 1_C} M \otimes_A C \to 0$$

*is exact.*

*So if $M$ has generators $\{m_i\}$ and relations $\sum a_{ij} m_i = 0$, then $M \otimes_A C$ has generators $(m_i \otimes 1)$ and relations $\sum g(a_{ij})(m_j \otimes 1) = 0$. Abuse notation by writing $m_i \otimes 1 = m_i$; this shows that $M \otimes_A C$ has the same generators and relations; the only thing is that $M \otimes_A C$ has coefficients in $C$ instead of just in $A$.*

*Even if we're dealing with vector spaces, it's useful because constructing the tensor product is intrinsic and choice-of-basis free.*

Now suppose that $A \xrightarrow{f} B$ is a ring homomorphism.

LEMMA 13.9. *(10.13) $B \otimes_A C = B \otimes_{f,A,g} C$ is a ring, and there is a commutative diagram*

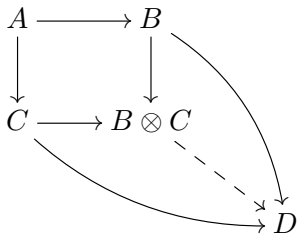
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle G} \\ C & \xrightarrow{F} & B \otimes_A C \end{array}$$

*where $G(b) = b \otimes 1_C = b \otimes 1$, and $F(c) = 1_B \otimes c$. Therefore, $f(a) \otimes 1 = 1 \otimes g(a)$. But these are tensors over $A$, and elements of $A$ can be moved across the tensor product symbol; if we had written $f$ and $g$ as inclusions, this would not be surprising.*

*Furthermore, this is universal: given a diagram*

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

*then there is a unique map* $\delta : B \otimes C \to D$ *making*




*commute.*

## Saturday optional lecture – November 3

Let $K$ be a field, $V$ a finite-dimensional $k$-vector space. If $V$ is a geometric object, $V = \mathbb{A}^n_k$, then these are functions on $V$. $k[V]$ is the ring of polynomial functions. The linear functions are the elements of $V^\vee$. So functions of higher degree are constructed by multiplying elements of $V^\vee$. The polynomials that are homogeneous of degree $n$ form a vector space $Symm^n(V^\vee)$.

Let's construct symmetric products in general. Let $A$ be a ring, $M$ an $A$-module. Look at

$$M^{\otimes n} M \otimes_A \cdots \otimes_A M$$

Then $TM = \oplus_{n\geq 0} M^{\otimes n}$ is a graded, associative $A$-algebra that is not commutative: even in degree 2, $m \otimes m' \neq m' \otimes m$. To make it commutative, quotient out by commutators. Define $Symm(M) = \bigoplus_{n\geq 0} Symm^n(M)$ to be $TM/I$, where $I$ is the 2-sided ideal generated by all elements of the form $m \otimes m' - m' \otimes m \in M^{\otimes 2}$.

Then $Symm(M)$ has the following properties: it's graded, in degree 0 it is $A$, in degree 1 it is $M$, it is generated in degree 1 by $M$, and has the following universal property:

- Given any commutative $A$-algebra $B$, and any $A$-linear map $\varphi : M \to B$, $\varphi$ extends to a unique $A$-algebra homomorphism $Symm(M) \to B$.

$Symm^n(M)$ is, by construction, a quotient of $M^{\otimes n}$. If $M$ is a free algebra with basis $e_1, \cdots, e_n$, then $Symm(M)$ is just the polynomial algebra $A[e_1, \cdots, e_n]$.

Over a field of characteristic zero, you can construct $Symm^n(M)$ as a submodule of $M^{\otimes n}$. If $A \supset \mathbb{Q}$ and $M$ is free, then $M^{\otimes n} \overset{\pi}{\twoheadrightarrow} Symm^n(M)$ splits, because over $\mathbb{Q}$ ever representation of the symmetric group $S_n$ is completely reducible. Say $e_1, \cdots, e_r$ is a basis of $M$. The set of all tensors $\{e_{i_1} \otimes \cdots \otimes e_{i_n}\}$ is an unordered basis of $M^{\otimes n}$, and $\{e_{i_1} \cdots e_{i_n} : i_1 \leq \cdots \leq i_n\}$ is an unordered basis of $Symm^n(M)$. Consider

$$\frac{1}{n!} \sum_{\sigma \in S_n} e_{\sigma(i_1)} \otimes \cdots \otimes e_{\sigma(i_n)}$$

This will give a basis of a submodule of $M^{\otimes n}$ that is isomorphic, under $\pi$, to $Symm^n M$. If you don't divide by $n!$, you still have an invariant object. Without assuming $A \supset \mathbb{Q}$, you can define $\Gamma^n M \hookrightarrow M^{\otimes n}$ to be the submodule of things that are invariant under $S_n$.

If $A \supset \mathbb{Q}$ then $\Gamma^n M \xrightarrow{\pi} Symm^n(M)$ is an isomorphism. Then $\bigoplus_n \Gamma^n M$ is a commutative $A$-algebra, but it is not always finitely generated (so it cannot be a polynomial ring).

This all works if $M$ is just locally free. This does not imply that you get a basis $e_1, \cdots, e_r$, however.

**Exterior product.** Define $\Lambda(M)$ to be the quotient $TM/J$, where $J$ is the two-sided ideal generated by all elements $(m \otimes m') + (m' \otimes m)$. So again, our ideal is generated by homogeneous elements of degree 2, and $\Lambda M$ is graded and associative, but *not* commutative. We denote the product by $\wedge$. So if $x, y \in \Lambda M$ are homogeneous of degree $p, q$ respectively, then $y \wedge x = (-1)^{pq} x \wedge y$.

$$\Lambda M = \bigoplus_n \Lambda^n M$$

If $M$ is locally free of rank $r$, then $\Lambda^n M$ is locally free of rank $\binom{r}{n}$. (In particular, it's equal to 0 for all $n > r$.)

If $M$ is free, with basis $(e_1, \cdots, e_r)$, then $\Lambda^n M$ is free, with basis $(e_{i_1} \wedge \cdots \wedge e_{i_n})$ where $i_1 < \cdots < i_n$. Note $e_i \wedge e_i = 0$, even in characteristic 2. As before, if $A$ contains a field of characteristic zero, then you can construct $\Lambda M$ as a subalgebra of $M^{\otimes n}$ by considering elements of the form

$$\frac{1}{n!} \sum_{\sigma \in S_n} (-1)^{sgn(\sigma)} e_{\sigma(i_1)} \otimes \cdots \otimes e_{\sigma(i_n)}$$

One way of seeing a locally free module $P$ over the ring $A$ is this: we have $s_1, \cdots, s_n \in A$ such that $(s_1, \cdots, s_n) = A$ and $S_\alpha^{-1} P$ is a free $S_\alpha^{-1} A$-module, of rank $r$, where $S_\alpha = \{s_\alpha^n : n \geq 0\}$. So we have a basis $(e_1^\alpha, \cdots, e_r^\alpha)$ of $S_\alpha^{-1} P$ over $S_\alpha^{-1} A$, and a basis $e_1^\beta, \cdots, e_r^\beta$ of $S_\beta^{-1} P$. Then over the ring $A[S_\alpha^{-1}, S_\beta^{-1}] \supset S_\alpha^{-1} A, S_\beta^{-1} A$ we have $e_i^\beta = \sum a_{ij}^{\beta\alpha} e_j^\alpha$ where $(a_{ij}^{\beta\alpha}) \in GL_r(A[S_\alpha^{-1}, S_\beta^{-1}])$. (So this tells you the $e^\beta$'s in terms of the $e^\alpha$'s, and the inverse of this matrix gives you the reverse.)

So the locally free module $P$ leads to a free rank $r$ module $S_\alpha^{-1} P$ over each ring $A[S_\alpha^{-1}]$ and a transition matrix $M^{\beta\alpha}$. We have compatibility: check $M^{\gamma\alpha} = M^{\gamma\beta} M^{\beta\alpha}$ (product of matrices).

Conversely, given a free module over each $A[S_\alpha^{-1}]$ and transition matrices, you can make a locally free module. (This is like a vector bundle.)

In these terms, each $\Lambda^n(S_\alpha^{-1}P)$ is free of rank $\binom{r}{n}$ over $A[S_\alpha^{-1}]$, and

$$\Lambda^n(S_\alpha^{-1}P) = S_\alpha^{-1}(\Lambda^n P)$$

(all tensor constructions commute with localization). There are transition matrices of size $\binom{r}{n}$ namely $\Lambda^n(M^{\beta\alpha})$.

Important special case: $n = r$, and $P$ is locally free of rank $r$. Then $S_\alpha^{-1}(\Lambda^r P)$ has a single generator $e_1^\alpha \wedge \cdots \wedge e_r^\alpha =: \eta_\alpha$, and $\eta^\beta = (\det M^{\beta\alpha} \cdot \eta^\alpha)$.

Suppose

$$0 \to P_2 \to P_1 \to P_0 \to 0$$

is an exact sequence of locally free modules, of rank $r_2, r_1, r_0$ respectively (so $r_1 = r_2 + r_0$). Then $\Lambda^{r_1} P_1 \cong \Lambda^{r_2} P_2 \otimes \Lambda^{r_0} P_0$. Why? We have $s_1, \cdots, s_m \in A$ such that $(s_1, \cdots, s_r) = A$ and each $S_\alpha^{-1}P_i$ is free of rank $r_i$. Then the transition matrices for $P_1$ are of the form

$$M^{1,\beta\alpha} = \begin{pmatrix} M^{2,\beta\alpha} & * \\ 0 & M^{0,\beta\alpha} \end{pmatrix}$$

where the labels $1, 2, 0$ refer to the modules $P_1, P_2, P_0$. This being zero in the lower left is "exactly what it means" for the sequence to be exact.

The transition functions (i.e. 1-dimensional transition matrices) for $\Lambda^{r_1} P_1$ are $\det(M^{1\beta\alpha})$. The transition functions for $\Lambda^{r_2} P_2$ are $\det(M^{2\cdot\beta\alpha})$ and $\det(M^{0,\beta\alpha})$ for $\Lambda^{r_0} P_0$. Observe

$$\det(M^{1,\beta\alpha}) = \det(M^{2,\beta\alpha}) \cdot \det(M^{0,\beta\alpha})$$

that follows from the block matrix form for $M^{1,\beta\alpha}$.

For locally free modules of rank 1, multiplying the transition functions is the same thing as tensoring the modules. (When it comes to taking determinants, tensor product *is* product.)

# Lecture 14: November 5

Suppose $A = k[x, y]$, and $\mathfrak{m} = (x, y)$. So $A/\mathfrak{m} = k$. Let $F_0$ be the free module on two generators $e_1, e_2$; there is a map $F_0 \xrightarrow{f_0} \mathfrak{m} \to 0$ that sends $e_1 \mapsto x$ and $e_2 \mapsto y$. There is a kernel $F_1$, so we get a short exact sequence

$$0 \to F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} \to \mathfrak{m} \to 0$$

$F_1$ is a free module of rank 1; let $g$ be the generator. So the map $f_1$ sends $g \mapsto xe_2 - ye_1$. Tensor with $k$: that is, apply the functor $- \otimes_A k$ to get a sequence

$$0 \to F_1 \otimes_A k \to F_0 \otimes_A k \to \underbrace{\mathfrak{m} \otimes_A k}_{\mathfrak{m}/\mathfrak{m}^2} \to 0$$

Recall, $M \otimes_A A/I \cong M/IM$. Note that $\dim F_1 \otimes_A k = 1$ $\dim F_0 \otimes_A k = 2$, and $\dim \mathfrak{m}/\mathfrak{m}^2 = 2$. So this sequence is not exact, and so $k$ is not a flat $A$-module.

Define $TM = \bigoplus_{n\geq 0} M^{\otimes n} := M \otimes_A \cdots \otimes_A M$. Then $TM$ is a graded, associative, non-commutative $A$-algebra. (In degree 0, it is $A$.) The exterior algebra is $\Lambda M := TM/J$, where $J$ is the 2-sided ideal generated by all elements of the form $m \otimes m$, where $m \in M$. $J$ is homogeneous by definition: it's generated by a bunch of things in degree 2. (This works in characteristic 2, as well.) Since $J$ is homogeneous, we have

$$\Lambda M = \bigoplus_{n\geq 0} \Lambda^n M$$

where $\Lambda^n M$ is the image of $M^{\otimes n}$ under the projection $TM \to TM/J$.

For example, if $n = 2$, $\Lambda^2 M$ is a quotient of $M^{\otimes 2}$, constructed by forcing every $m \otimes m$ to be equal to 0. If $m = x + y$, then

$$0 = (x + y) \otimes (x + y) = x \otimes x + y \otimes y + x \otimes y + y \otimes x$$

So in $\Lambda^2 M$ we get

$$0 = x \otimes y \pmod{J} + y \otimes x \pmod{J}$$

Then $TM$ has an associative multiplication in $\Lambda M$ by $\wedge$. So we have

$$0 = x \wedge y + y \wedge x.$$

So far, this has all worked in characteristic 2, or in $\mathbb{Z}$, etc. But, if 2 is invertible, then forcing $m \otimes m = 0$ is the same as forcing every $m \otimes m' + m' \otimes m = 0$. Also, if $\frac{1}{2} \in A$, then we can construct $\Lambda^2 M$ as a **sub**module of $M^{\otimes 2}$: as the set of elements $z$ such that $\sigma(z) = (-1)^{sgn(\sigma)} z$ for all $\sigma \in S_2$ (the symmetric group). More generally, if $\frac{1}{n!} \in A$, then we can construct $\Lambda^n M \hookrightarrow M^{\otimes n}$ as

$$\{z \in M^{\otimes n} \,:\, \sigma(z) = (-1)^{sgn(\sigma)} z \;\forall \sigma \in S_n\}$$

For any $A$-algebra $B$,

$$(\Lambda^n M) \otimes_A B \cong \Lambda^n (M \otimes_A B)$$

but $(\Lambda^2 M) \otimes_{\mathbb{Z}} \mathbb{F}_2$ might fail to be $\Lambda^2(M \otimes_Z \mathbb{F}_2)$. Also, $S^{-1}M = M \otimes (S^{-1}A)$, so $S^{-1}(\Lambda^n M) = \Lambda^n (S^{-1} M)$.

What happens when $M$ is free, say of rank $r$? Say $(e_1, \cdots, e_r)$ is a basis of $M$. Then

$$(e_{i_1} \wedge \cdots \wedge e_{i_n})_{i_1 < \cdots < i_n}$$

is a basis of $\Lambda^n M$, because $m \wedge m = 0$ for all $m \in M$.

If $x \in \Lambda^p M$ and $y \in \Lambda^q M$, then $x \wedge y$, $y \wedge x \in \Lambda^{p+q} M$, and $y \wedge x = (-1)^{pq}(x \wedge y)$; i.e. $\Lambda^n$ is free of rank $\binom{n}{r}$. In particular, $\Lambda^r M$ is free of rank 1.

For example, if I have a homomorphism $\varphi : M \to N$ of modules, then $\Lambda^n M \overset{\Lambda^n \varphi}{\to} \Lambda^n N$. In particular, if $M = N$ is free of rank $r$, then $\Lambda^r \varphi$ is a map from a free rank-1 module to itself, so $\Lambda^r \varphi \in A$. In particular, $\Lambda^r \varphi = \det \varphi$.

Suppose $\varphi : M \to M$ is a homomorphism where $M$ is free of rank $r$. So we can pick a basis of $M$, and represent $\varphi$ by an $r \times r$ matrix. Then $\det \varphi = \det(\text{matrix})$. Given

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M \\ {\scriptstyle \psi\varphi}\downarrow & \swarrow{\scriptstyle \psi} & \\ M & & \end{array}$$

you get $\Lambda^n(\psi \circ \varphi) = \Lambda^n\psi \circ \Lambda^n\varphi$ for any $n$. So $\det(\psi \circ \varphi) = \det\psi \det\varphi$.

Now suppose that $M$ is locally free of rank $r$. Then $\Lambda^n M$ is locally free of rank $\binom{r}{n}$: this is because $S_i^{-1}(\Lambda^n M) = \Lambda^n(S_i^{-1}M)$. Say $S_\alpha^{-1}M$ has a basis $(e_1^\alpha, \cdots, e_r^\alpha)$, and $S_\beta^{-1}M$ has a basis $(e_1^\beta, \cdots, e_n^\beta)$. Then

$$e_i^\beta = \sum_{j=1}^{r} u_{ij}^{\beta\alpha} e_j^\alpha$$

for $u_{ij}^{\beta\alpha} \in A[S_\alpha^{-1}, S_\beta^{-1}]$. I can express the $e_i^\alpha$'s in terms of the $e_i^\beta$'s as well, so the matrix $(u_{ij}^{\beta\alpha}) \in GL_r([S_\alpha^{-1}, S_\beta^{-1}])$ is invertible.

This is like a manifold: the transition matrices are like transition maps in chart-land. Analogously, we need $(i_{ij})^{\gamma\alpha} = (u_{ij}^{\gamma\beta}) \cdot (u_{ij}^{\beta\alpha})$.

# Lecture 15: November 7

Last time, we were discussing exterior products. Let $M$ be a locally free $A$-module of rank $r$. This means that there exist elements $s_1, \cdots, s_m \in A$ such that

- $(s_1, \cdots, s_m) = A$, and
- each $S_\alpha^{-1}M$ is a free $S_\alpha^{-1}A$-module of rank $r$.

Then $\Lambda^n M$ is locally free of rank $\binom{r}{n}$. Each $S_\alpha^{-1}(\Lambda^n M) = \Lambda^n(S_\alpha^{-1}M)$. If $(e_1^\alpha, \cdots, e_r^\alpha)$ is a basis of $S_\alpha^{-1}M$, and $(e_1^\beta, \cdots, e_r^\beta)$ is a basis of $S_\beta^{-1}M$ then we can write

$$e_j^\beta = \sum u_{ji}^{\beta\alpha} e_i^\alpha$$

where $(u_{ji}^{\beta\alpha}) \in GL_r(A[S_\alpha^{-1}, S_\beta^{-1}])$. Note that $S_\alpha^{-1}A = A[s_\alpha^{-1}]$ (where $s_\alpha$) is a single element.

If $A = k[V]$, if $u_\alpha = V - (s_\alpha = 0)$ then $S_\alpha^{-1}A = k[u_\alpha]$. $V = \bigcup U_\alpha$ and $A[s_\alpha^{-1}, s_\beta^{-1}] = k[u_\alpha \cap u_\beta]$.

$\Lambda^n(S_\alpha^{-1}M)$ has a basis

$$(e_{i_1}^\alpha, \cdots, e_{i_n}^\alpha)_{i_1 < \cdots < i_n}$$

and similarly for $\Lambda^n(S_\beta^{-1}M)$.

The transition matrix is $\Lambda^n(u_{ji}^{\beta\alpha})$. If you take a representation of $GL_r$, you can take the exterior power, and get another representation of dimension $\binom{n}{r}$, where the entries are polynomials in the entries of the original matrix of the representation.

In particular, take $n = r$. Then $\Lambda^r M$ is locally free of rank 1, a.k.a. *invertible*. Define $\Lambda^r M =: \det M$. The transition matrices of $\det M$ are determinants of the transition matrices of the free local bits.

LEMMA 15.1. *Define the* dual $M^\vee$ *of* $M$ *by*

$$M^\vee = \mathrm{Hom}(M, A)$$

*There is a natural homomorphism* $M \to M^{\vee\vee}$ *which is an isomorphism if* $M$ *is locally free of finite rank.*

With modules that are not locally free, this is not necessarily true. For example, take $A = \mathbb{Z}$ and $M = \mathbb{Z}/2$. Then $M^\vee = 0$.

PROPOSITION 15.2. *If* $M$ *is locally free, then for any* $N$, $\mathrm{Hom}(M, N) \cong M^\vee \otimes N$.

For any $M$, there is a natural map $A \to \mathrm{Hom}(M, M)$ given by $a \mapsto$ multiplication by $a$.

If $M$ is locally free of rank 1, then $A \xrightarrow{\varphi} \mathrm{Hom}(M, M) \cong M^\vee \otimes M$ is an isomorphism. So "tensoring with the dual" produces the inverse of a locally free, rank-1 module $M$. It's enough to prove that $\varphi$ is an isomorphism locally, i.e. over each ring $S_\alpha^{-1}A$. Now $S_\alpha^{-1}M$ has a generator $e^\alpha$, and $\varphi(x)(e^\alpha) = x \cdot e^\alpha$. So $\varphi(1)$ is the identity, and $\varphi$ is an isomorphism.

So the isomorphism classes of locally free modules of rank 1 form a group under $\otimes$.

Suppose we have $\psi : M \to N$, a homomorphism of locally free modules of finite rank. This induces $\Lambda^n\psi : \Lambda^n M \to \Lambda^n N$, for all $n$. Assume on each chart that $M$ and $N$ are free. Then $\psi$ can be represented by a matrix. Note that if $S_\alpha^{-1}M$ and $S_\alpha^{-1}N$ are both free, then we can choose bases and represent $S_\alpha^{-1}\psi$ by a matrix, over the ring $S_\alpha^{-1}A$.

EXERCISE 15.3. Work out transition matrices for $\psi$. Describe matrices for the locally free modules $\mathrm{Hom}(M, N)$ and $M^\vee \otimes N$, and observe that they are the same, thereby confirming that $\mathrm{Hom}(M, N) \cong M^\vee \otimes N$.

EXERCISE 15.4. If

$$0 \to P_2 \to P_1 \to P_0 \to 0$$

is exact, with $P_0$ and $P_1$ locally free of finite rank, then $P_2$ is also locally free of rank $= rank(P_1) - rank(P_0)$.

The existence of an exact sequence like this implies the following: if $S_\alpha^{-1}P_2$ ad $S_\alpha^{-1}P_0$ are free for all $\alpha$, then $S_\alpha^{-1}P_1$ is free (i.e. local bases of $P_0$ and $P_2$ combine to give a local basis of $P_1$), and transition matrices will be of the form

$$\begin{pmatrix} X & * \\ 0 & Y \end{pmatrix}$$

where $X$ is a transition matrix for $P_2$, $Y$ is a transition matrix for $P_0$, and $*$ is unknown. Therefore, $\det P_1 \cong (\det P_0) \otimes (\det P_2)$, since the determinant of the matrix above is $\det(X)\det(Y)$.

For locally free of rank 1, the product of transition functions is the transition function of the tensor product.

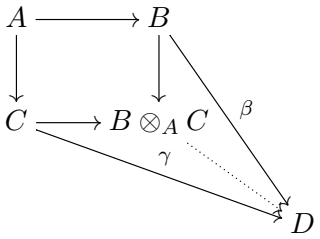
For any finite exact sequence of locally free modules, the alternating product of the determinants is zero.

Now: $M$ is an $A$ module, $B$ is an $A$-algebra. Then $B \otimes_A M$ is then a $B$-module. Then $\Lambda^n(B \otimes_A M) \cong B \otimes_A (\Lambda^n M)$, where the first wedge is over $B$, and the second is over $A$. (In theory, the notation $\Lambda^n M$ should also specify what ring the exterior product is being taken over.)

If $B, C$ are $A$-algebras, then $B \otimes AC$ is a ring, fitting in a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow{\scriptstyle b\mapsto b\otimes 1} \\ C & \xrightarrow{c\mapsto 1\otimes c} & B \otimes_A C \end{array}$$

This makes sense because elements of $A$ are allowed to move across the $\otimes$ sign: $(ab) \otimes c = b \otimes (ac)$. If $D$ is a ring fitting in a commutative diagram




of solid arrows, then there is a unique map $B \otimes_A C \to D$ as shown, satisfying $\varphi(b \otimes c) = \beta(b)\gamma(c)$.

For example, suppose $A = k$, $B = k[V]$, $C = k[W]$. Then $B \otimes_A C = k[V \times W]$. All of these things are symmetric: $B \otimes C \cong C \otimes B$ canonically, and $V \times W = W \times V$. But you can also read this asymmetrically: suppose $A = k$, $B = L$, $C = k[V]$. Then $B \otimes AC = L[V]$ (where I regard $V$ as being defined over $L$).

For example, let $A = \mathbb{Z}$, $B = \mathbb{Z}/p$, and $C = \mathbb{Z}[X, Y]/(Y^2 + X^3 + X + 1 = 0)$. Then $Bts_A C = (\mathbb{Z}/p)[X, Y]/(Y^2 + X^3 + X + 1 = 0)$. Tensor products give language for extending scalar fields, and for reduction modulo $p$.

It's also possible to do algebraic geometry over a non-algebraically closed field. But that's more a task for scheme theory.

# Lecture 16: November 9

**Vector fields and differentials on open subsets $U$ of $\mathbb{R}^n$.** Let $A$ be the ring of $C^\infty$ functions $U \to \mathbb{R}$. A vector field on $U$ is a derivation $X : A \to A$: $X(f)$ is a function

- $X(f+g) = X(f) + X(g)$
- $X(\lambda) = 0$ if $\lambda \in \mathbb{R}$
- (Leibniz rule) $X(fg) = fX(g) + gX(f)$

For example, if $x_1, \cdots, x_n$ are coordinates in $U$ then $\frac{\partial}{\partial x_i}$ is a vector field, and the vector fields in $U$ form a free $A$-module with basis $\left(\frac{\partial}{\partial x_1}, \cdots, \frac{\partial}{\partial x_n}\right)$. Recall that usually you define a tangent vector at $P$ to be an equivalence of maps $\gamma : (-\delta, \delta) \to U$, with $\gamma(0) = P$, and $\gamma \sim \widetilde{\gamma}$ if $\gamma'(0) = \widetilde{\gamma}'(0)$. The tangent space is a vector space, and then the tangent bundle is the union of all vector spaces, topologized in a way that makes it a vector bundle over $U$. So if $U \subset \mathbb{R}^n$, then we get a free module. The dual of this module is the module of 1-forms on $U$.

If $S \hookrightarrow M$ is a submanifold, we have an exact sequence

$$0 \to T_s \to T_M|_S \to N_{S/M} \to 0$$

where $N_{S/M}$ is the *normal bundle*, and it is defined this way, i.e. as the quotient $T_M|_S/T_S$. There is also a dual sequence

$$0 \leftarrow T_s^* \leftarrow T_M^*|_S \leftarrow N_{S/M}^* \leftarrow 0$$

In the Riemannian world, you can construct $N \subset T_M|_S$ as the orthogonal complement of $T|_S$. But in general, this sequence doesn't split.

Take the special case where $M = S \times S$, and $S \hookrightarrow M$ is the diagonal $\Delta$. Then

$$T_M = pr_1^* T_S \oplus pr_2^* T_S$$

and we get a sequence

$$0 \to T_\Delta = T_S \to T_S \oplus T_S \to N_{\Delta/M} \to 0$$

and the normal bundle is isomorphic to the tangent bundle. Also $N_\Delta^\vee / S \times S = \Omega_S^1$.

**Back to algebra.** Suppose $A = k[V]$, and suppose $W \hookrightarrow V$ is a subvariety. Then $W$ is defined by an ideal $I$ of $A$. Define the conormal bundle[2] of $W$ in $V$ to be $I/I^2$. Define the normal bundle

$$N_{W/V} = (I/I^2)^\vee = \mathrm{Hom}_{A/I}(I/I^2, A/I)$$

(where $A/I = k[W]$). (Note that $(I/I^2)^{\vee\vee}$ might not be the same as $I/I^2$.)

[2] Just a module, not necessarily locally free!

Now we shall construct $\Omega^1_V$ as the conormal bundle of $\Delta$ inside $V \times V$. So, start with a ring $k$ and a $k$-algebra $A$. We know that $A \otimes_k A$ is a ring fitting in

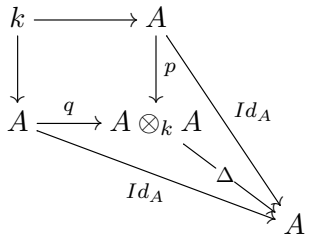
$$\begin{array}{ccc} k & \longrightarrow & A \\ \downarrow & & \downarrow p \\ A & \xrightarrow{q} & A \otimes_k A \end{array}$$

where $p(a) = a \otimes 1$ and $q(a) = 1 \otimes a$. So $A \otimes_k A$ is naturally an $A$-algebra, in two different ways. If $k$ is a field, and $A = k[V]$, then $A \otimes_k A = k[V \times V]$, and $p$ and $q$ correspond to the two projections $V \times V \to V$. Furthermore, $p$ and $q$ are equal after modding out by $I$:

$$\begin{array}{ccc} (A \otimes A)/I & = & A \\ \uparrow & & \uparrow Id_A \\ A \otimes A & \underset{q}{\overset{p}{\leftleftarrows}} & A \end{array}$$

Inside $V \times V$ there is a diagonal $\Delta \hookrightarrow V \times V$, and $\Delta \overset{\cong}{\to} V$ under each projection. Because $\Delta$ is a subvariety of $V \times V$, $k[\Delta]$ must be a quotient of $k[V \times V]$: that is, $k[\Delta] \cong (k[V] \otimes_k k[V])/I$ for some ideal $I = \ker \Delta$.

The diagonal map $\Delta$ fits in a diagram:




(Abuse of notation warning: $\Delta$ refers both to the diagonal map and to the diagonal set.)

Now define $\Omega^1_{A/k} := I/I^2$, an $A$-module, as the module of *Kähler differentials.*

Definition 16.1. If $M$ is an $A$-module, then a $k$-derivation for $A$ to $M$ is a map $D : A \to M$. $D$ is $k$-linear, additive, and

$$D(fg) = f \cdot D(g) + g \cdot D(f) \ \forall f, g \in A$$
$$D(\lambda) = 0 \ \forall \lambda \in k$$

These form an $A$-module, $Der_k(A, M)$: that is, $(aD)(b) := a \cdot (D(b))$.

Lemma 16.2. *(13.4) The map $d = d_{A/k} : A \to \Omega^1_{A/k}$ given by $d(a) = (a \otimes 1 - 1 \otimes a)$, modulo $I^2$, is a $k$-derivation.*

(Notice that $d(a) \in I$, because $\Delta(d(a)) = 0$.)

*Proof.* Exercise. ○

This $d$ is the algebraic version of exterior differentiation from functions to 1-forms.

PROPOSITION 16.3. *(13.6) $d$ is universal in the following sense: given any $M$ and any $k$-derivation $D : A \to M$ there is a unique $A$-homomorphism $f : \Omega^1_{A/k} \to M$ such that*

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega^1_{A/K} \\ & \searrow^{D} & \downarrow f \\ & & M \end{array}$$

*commutes. In other words,*

$$Der_k(A, M) \cong \mathrm{Hom}_A(\Omega^1_{A/k}, M).$$

*Proof.* Suppose we are given $D : A \to M$. Then define $\varphi : A \otimes_k A \to A \oplus M$ by $\varphi(x \otimes y) = (xy, x \cdot D(y))$. Define a ring structure on $A \oplus M$:

$$(a, m)(b, n) = (ab, an + bm).$$

so that $M$ is an ideal in $A \oplus M$ and $M^2 = 0$. ($A \oplus M$ is the symmetric algebra $Symm(M)$ modulo all terms of degree $\geq 2$.) Then $\varphi$ is a $k$-algebra homomorphism, and $\varphi(I) \subset M$. So $\varphi(I^2) = 0$. So $\varphi$ induces $\overline{\varphi} : (A \otimes_k A)/I^2 \to A \oplus M$. Now define $f : \Omega^1_{A/k} \to M$ as the composite of

$$\Omega^1_{A/k} = I/I^2 \hookrightarrow (A \otimes_k A)/I^2 \xrightarrow{\beta\varphi} A \oplus M \xrightarrow{pr_2} M$$

It is easy to see that $f \circ d = D$, and $f$ is the only such. ○

LEMMA 16.4. *(13.7) If $A = k[X]$, then $\Omega^1_{A/k} = A \cdot dX$ (free of rank 1).*

*$X$ is just a variable, not a variety.*

*Proof.* $A \otimes_k A \cong k[X_1, X_2]$ where $X_1 = X \otimes 1$ and $X_2 = 1 \otimes X$. The kernel $I$ of the diagonal is generated by $X_2 - X_1$. So $\Omega^1 = I/I^2$ is generated by the class of $X_2 - X_1 = dX$, since $d(a) = 1 \otimes a - a \otimes 1$.

Now I need to show that there are no relations. There is a derivation $D = \frac{\partial}{\partial X} : A \to A$. Then $D(X) = 1$. There exists $f : \Omega^1_{A/k} \to A$ such that $f(dX) = D(X) = 1$. If $a \cdot dX = 0$ we'd get $0 = f(a \cdot dX) = a \cdot f(dX) = a$.

○

**Correction to example sheet 2, question #11.** If $A$ is Noetherian, we've proved every $I = \bigcap_{i=1}^{m} Q_i$ for primary $Q_i$. $Q$ primary implies $\sqrt{Q}$ is prime, but the converse is not true. We deduced that every radical ideal $J$ has a unique irredundant description $J = \bigcap P_i$ for $P$ prime. So closed subsets of $\mathbb{A}_k^n$ are uniquely unions of irreducible pieces. Now allow $I$ to be arbitrary.

LEMMA. If $Q_1, \cdots, Q_r$ are primary, with $\sqrt{Q_i} = P$ for all $i$, then $\bigcap Q_i$ is also $P$-primary.

So any $I$ is $\bigcap Q_i$ with all $\sqrt{Q_i}$ distinct, and moreover no $Q_i \supset_{j \neq i} Q_j$ (because then you could just omit it). Such a decomposition is irredundant. If $I = \sqrt{I}$, then we could write $I$ as an intersection of primes, and the decomposition would be unique. But if $I \neq \sqrt{I}$ then $I$ can have distinct irredundant decompositions (uniquness can fail).

THEOREM. In any irredundant decomposition $I = \bigcap Q_i$, the set $\{\sqrt{Q_i}\}$ equals the set of ideals $\{\sqrt{(I : x)}\}$ which are prime. Here, $x$ ranges over all elements of $A$ and

$$(I : x = \{y \in A \,:\, yx \in I\})$$

Consequence: if $I = \bigcap_i Q_i = \bigcap_j Q'_j$ are two irredundant decompositions, then

$$\{\sqrt{Q_i}\} = \{\sqrt{Q'_j}\}$$

(that is, the lists of radicals are the same). This is stronger than the statement that radical ideals are uniquely an irredundant intersection of primes. The set $\{\sqrt{Q_i}\}$ is the set of prime ideals belonging to $I$. Some are minimal; equivalently, they are minimal amongst the set of all prime ideals that contain $I$. The others are *embedded*.

PROPOSITION. Suppose that $I = \bigcap Q_i$ is an irredundant expression. Suppose that $P_i = \sqrt{Q_i}$. (By the theorem, $P_i = \sqrt{(I : x_i)}$ for some $x_i \in A$.) Then

$$\bigcup P_i = \{x \in A \,:\, (I : x) \supsetneq I\} = \{x \in A \,:\, x \text{ is a zero-divisor} \pmod{I}\}$$

$\{$ zero-divisors in $A$ $\}$ $= \bigcup P$ where $P$ are prime ideals belonging to 0. (Find this in Atiyah-Macdonald.)

(See Atiyah-Macdonald pp. 52-53.)

For example, take $A = k[x, y]/(x^2, xy)$. This is the coordinate ring of the $y$-axis together with some embedded noise at the origin. The latter can be seen algebraically but not geometrically. The moral is that radical ideals give you things you can see, but more information is hidden in non-radical ideals. In $k[x, y]$, $(x^2, xy) = (x) \cap (x, y)^2$ (note $(x, y)$ is maximal so its square is primary). So in $A$, $(0) = (x) \cap (x, y)^2$, and the set of zero-divisors in $A$ is $(x) \cup (x, y) = (x, y)$. Indeed, every $f \in A$ with zero constant term is annihilated by $x$.

Here $nil(A) = (x)$. Question #11 implies that $\bigcup P_i = (x)$, but we've just shown that's not the case. The correct form of the question should be the statement of the proposition above.

**Locally free modules.** Let $N$ be any $A$-module, and $M$ a locally free of finite rank, finitely-generated module over $A$.

PROPOSITION.
$$M \otimes N \cong \mathrm{Hom}(M^\vee, N)$$

The point is to construct a map $\alpha : M \otimes N \to \mathrm{Hom}(M^\vee, N)$, and show it's an isomorphism after localising. Send
$$m \otimes n \overset{\alpha}{\mapsto} (\varphi : \lambda \mapsto \lambda(m) \cdot n)$$
where $\lambda \in M^\vee$. You have to check that this is well-defined, or equivalently show that this comes from a bilinear map $\widetilde{\alpha} : M \times N \to \mathrm{Hom}(M^\vee, N)$.

CLAIM 16.1. *If $S \in A$, $S = \{s^n : n \geq 0\}$ such that $S^{-1}M$ is a free $S^{-1}A$-module of finite rank, then $S^{-1}\alpha$ is an isomorphism.*

CLAIM 16.2.
$$S^{-1}(M^\vee) = (S^{-1}M)^\vee$$
*if $M$ is finitely generated.*

*Proof.* It's easy to show that $S^{-1}(M^\vee) \subset (S^{-1}M)^\vee$. So start with $\varphi : S^{-1}M \to S^{-1}A$; we want to show this is a homomorphism $M \to A$, possibly with denominators. Say $M$ is generated by $m_1, \cdots, m_n$ (we assumed $M$ was finitely presented; hence, it's finitely generated). $\varphi(m_i) = \frac{a_i}{s_i}$. Write $t = s_1 \cdots s_n$ be a product of denominators. Then
$$t\varphi(m_i) = s_1 \cdots \widehat{s_i} \cdots s_n$$
where $a_i \in A$. Define $\psi : M \to A$ where $\psi(m_i) = s_1 \cdots \widehat{s_i} \cdots a_i$. Then $\psi = t\varphi$, and $\varphi = t^{-1}\psi$. So $\psi \in M^\vee$, $\varphi \in S^{-1}(M^\vee)$. ○

Pick a basis $(e_1, \cdots, e_n)$ of $S^{-1}M$ and take the dual basis $(e_1^\vee, \cdots, e_n^\vee)$ of $S^{-1}(M^\vee) = (S^{-1}M)^\vee$. You finish.

**Tensor products.**

PROPOSITION. If $M, N$ are locally free of the same *finite* rank, then any surjective homomorphism $M \to N$ is an isomorphism.

*Proof.* We have a short exact sequence
$$0 \to K \to M \overset{\varphi}{\to\to} N \to 0$$
(where $K$ is the kernel). We need to show that $K = 0$. A module is zero if it is everywhere locally zero: that is, if there exist $s_1, \cdots, s_r \in A$ such that $(s_1, \cdots, s_r) = A$ and $S_i^{-1}K = 0$ for all $S_i = \{s_i^n : n \geq 0\}$. We may assume $S_i^{-1}M$ and $S_i^{-1}N$ are free over $S_i^{-1}A$. Suppose that $s_1, \cdots, s_r \in A$ such that each $S_i^{-1}A$ is free, and suppose there are $t_1, \cdots, t_n \in A$ such that $T_j^{-1}N$ is free. Now $(s_1, \cdots, s_n) = A$, and $(t_1, .., t_n) = A$. $A = A \cdot A = (s_1, \cdots, s_m)(t_1, \cdots, t_n) = (s_i t_j)$. $M[s_i^{-1}]$ is $A[s_i^{-1}]$-free, so $M[s_i^{-1}][t_j^{-1}]$ is $A[s_i^{-1}][t_j^{-1}]$-free (if it's free, it's still free if you invert something else). So $M[(s_i t_j)^{-1}]$ is $A[(s_i t_j)^{-1}]$-free. ○

Suppose I have ring homomorphisms $A \to B \to C$ and an $A$-module $M$. Then I claim

$$C \otimes_A M \cong C \otimes_B (B \otimes_A M)$$

(extending scalars all at once is the same as extending scalars in two steps).

# Lecture 17: November 12

Let's generalize the last example from last time.

Proposition 17.1. *If $A = k[X_1, \cdots, X_n]$ then $\Omega^1_{A/k} = \bigoplus_{i=1}^n A\ dX_i$.*

*Proof.* Remember that $\Omega_{A/k}$ was constructed by looking at the diagonal. Define $Y_i = X_i \otimes 1$ and $Z_i = 1 \otimes X_i$. So $A \otimes_k A = k[Y_1, \cdots, Y_n, Z_1, \cdots, Z_n] = k[\mathbb{A}^n \times \mathbb{A}^n]$. Let $I$ be the ideal of the diagonal, generated by the elements $(Y_1 - Z_1, \cdots, Y_n - Z_n)$.

Then $\Omega^1_{A/k} = I/I^2$ and we have a map $d : A \to \Omega^1_A$, where $d(a) = 1 \otimes a - a \otimes 1$ (modulo $I^2$). So $dX_i = Z_i - Y_i \pmod{I^2}$. So $dX_1, \cdots, dX_n$ generate $\Omega^1_{A/k}$ as an $A$-module.

Now we show that there are no relations. Suppose $\sum a_i\ dX_i = 0$. Consider $\frac{\partial}{\partial X_1} : A \to A$, a $k$-derivation. We get $f : \Omega^1_{A/k} \to A$. Then

$$f(dX_i) = \frac{\partial}{\partial X_1}(X_i) = \delta_{1i}$$

(the Kronecker delta). But $f(\sum a_i\ dX_i) = 0$ so $a_1 = 0$. Similarly, every $a_j = 0$. ○

Need to show that the $dX_i$ generate $I/I^2$ and are linearly independent. For the first, find generators of $A \otimes A \supset I$. Use the definition of $I$ to show that an arbitrary element of $I$, written in terms of these generators, is a linear combination of $X_i \otimes 1 - 1 \otimes X_i = dX_i$.

For linear independence, if $\sum a_i\ dX_i = 0$, apply $f_j : \Omega^1 \to A$ defined by $da \mapsto \frac{\partial}{\partial X_j} a$.

Lemma 17.2. *(13.8) For all $k$-modules $M$ and an $A$-module $N$, there is a natural isomorphism*

$$\mathrm{Hom}_k(M, N) \xrightarrow{\cong} \mathrm{Hom}_A(M \otimes_k A, N)$$

Theorem 17.3 (First fundamental exact sequence). *(13.9) Suppose that $B$ is an $A$-algebra. Then there is an exact sequence of $B$-modules*

$$\Omega^1_{A/k} \otimes_A B \xrightarrow{v} \Omega^1_{B/k} \xrightarrow{u} \Omega^1_{B/A} \to 0$$

*where $u$ and $v$ are defined by:*

$$v(d_{A/k}(a) \otimes b) = b\ d_{B/k}(a)$$

$$u(b\ d_{B/k}(b')) = b\ d_{B/A}(b')$$

*Moreover, $v$ has a left inverse (i.e. the sequence splits) $\iff$ for all $B$-modules $N$, every $k$-derivation $D : A \to N$ can be extended to a $k$-derivation $B \to N$.*

*Proof.* Take $u, v$ as given, and then verify exactness. The sequence is exact iff, for all $B$-modules $N$, the sequence

$$0 \to \mathrm{Hom}_B(\Omega^1_{B/A}, N) \xrightarrow{\alpha'} \mathrm{Hom}_B(\Omega^1_{B/k}, N) \xrightarrow{\beta'} \mathrm{Hom}_B(\Omega^1_{A/k} \otimes B, N)$$

is exact (Lemma 10.6). By Lemma 13.8, the last term is $\mathrm{Hom}_A(\Omega^1_{A/k}, N)$, so we can rewrite the sequence as

$$0 \to \mathrm{Der}_A(B, N) \xrightarrow{\alpha} \mathrm{Der}_k(B, N) \xrightarrow{\beta} \mathrm{Der}_k(A, N)$$

$\alpha$ is an injection: it takes an $A$-derivation (which by definition kills $A$) and regards it as a $k$-derivation. $\beta$ is just restriction. If $D \in \ker(\alpha)$, then $D$ (as an element of $\mathrm{Der}_A(B, N)$) kills $A$, and hence restricts to the zero derivation in $\mathrm{Der}_k(A, N)$. So $\ker \beta = \mathrm{im}\, \alpha$.

For the second statement, $v$ has a left inverse $\iff$ for all $B$-modules $N$, the map $\beta'$ is surjective (general nonsense about modules). $\beta'$ is surjective $\iff$ $\beta$ is surjective, which is exactly the condition given.

○

Use 10.6 to turn the (proposed) exact sequence of modules into an exact sequence of $\mathrm{Hom}(*, N)$. Use definitions to turn this into a sequence of $\mathrm{Der}(*, N)$.

Corollary 17.4. *(13.10)*

$$\Omega^1_{A/k} \otimes_A B \xrightarrow{v} \Omega^1_{B/k}$$

*is an isomorphism* $\iff$ *every $k$-derivation $D : A \to N$ has a unique extension to $B$.*

Theorem 17.5 (Second fundamental exact sequence). *(13.11) Suppose $B = A/J$. Then there is an exact sequence of $B$-modules*

$$J/J^2 \xrightarrow{\delta} \Omega^1_{A/k} \otimes_A B \xrightarrow{v} \Omega^1_{B/k} \to 0$$

*where $\delta(x) = d_{A/k}(x) \otimes 1 = d_{A/k}(x) \pmod J$.*

*Proof.* Take $\delta$ as given. Then exactness holds $\iff$ for all $B$-modules $N$, the sequence

$$0 \to \mathrm{Hom}_B(\Omega^1_{B/k}, N) \to \mathrm{Hom}_B(\Omega^1_{A/k} \otimes_A B, N) \to \mathrm{Hom}_B(J/J^2, N)$$

is exact. This is the same as

$$0 \to \mathrm{Der}_k(B, N) \to \underbrace{\mathrm{Hom}_A(\Omega^1_{A/k}, N)}_{\mathrm{Der}_k(A,N)} \to \mathrm{Hom}_A(J, N)$$

So we need exactness of

$$0 \to \mathrm{Der}_k(B, N) \xrightarrow{\gamma} \mathrm{Der}_k(A, N) \xrightarrow{\varepsilon} \mathrm{Hom}_A(J, N)$$

$\gamma$ is defined as

$$(B \xrightarrow{D} N) \xmapsto{\gamma} (A \to B \xrightarrow{D} N)$$

Suppose $\gamma(D) = 0$. Then $D|_A = 0$, and (since $B = A/J$) $D : B \to N$ is also zero. So $\gamma$ is injective.

I need to verify $\operatorname{im}\gamma = \ker\varepsilon$. If $D : A \to N$ is a $k$-derivation, then $D$ kills $J^2$ because $J \cdot N = 0$. So $\varepsilon(D)$ is just $D|_J$: the $k$-derivation $D$ becomes $A$-linear when restricted to $J$. $D$ lies in $\ker\varepsilon$ iff $D$ annihilates $J$, iff $D$ lies in $\operatorname{im}(\delta)$. ○

Basically the same as the first fundamental exact sequence. Use 10.6 to transform this into a problem about $\operatorname{Hom}(*, N)$; rewrite in terms of $\operatorname{Der}(*, N)$ and check exactness there.

COROLLARY 17.6. *(13.12) If $B = k[X_1, \cdots, X_n]/(f_1, \cdots, f_n)$, then*

$$\Omega^1_{B/k} = \bigoplus_{i=1}^{n} B\ dX_i/(df_j = 0\ \forall j)$$

*where $df_j = \sum_{I=1}^{n} \frac{\partial f_j}{\partial x_i}\ dX_i$.*

In the language of the previous theorem, $A = k[X_1, \cdots, X_n]$ and $J = (f_1, \cdots, f_n)$; $\bigoplus_{i=1}^{n} B\ dX_i = \Omega^1_{A/k} \otimes_A B$ and the ideal $(df_j = 0\ \forall j)$ is $\operatorname{im}(\delta)$.

LEMMA 17.7. *(13.13)*

$$\Omega^1_{(S^{-1}A)/k} = S^{-1}(\Omega^1_{A/k})$$

*Proof.* Apply Theorem 13.9 with $B = S^{-1}A$. ○

LEMMA 17.8. *(13.14) A ~~finitely generated~~ **finite** field extension $K/k$ is algebraic and separable $\iff$ $\Omega^1_{K/k} = 0$.*

(The proof given only addresses the case when $K/k$ is a finite extension.)

*Proof.* If $K/k$ is finite, algebraic, and separable, then by the primitive element theorem, $K = k(\alpha) \cong k[X]/(f)$ and then $\Omega^1_{K/k} = K\ dX\ (\text{mod } \frac{\partial f}{\partial X} = 0)$. This is zero since $\frac{\partial f}{\partial X}|_{X=\alpha} \neq 0$ (this is by separability – write $f = \prod(x - \theta_i)$ in some extension field; differentiate, remembering that $\theta_i \neq \theta_j$).

Conversely, suppose $\Omega^1_{K/k} = 0$. We have $k \subset L \subset K$, where $L = k(x_1, \cdots, x_r)$ is purely transcendental, and $K/L$ is algebraic. We have an exact sequence

$$\Omega^1_{L/k} \otimes K \to \underbrace{\Omega^1_{K/k}}_{0} \to \Omega^1_{K/L} \to 0$$

So $K/L$ is separable and algebraic, $K = L(\alpha)$, where $\alpha$ has minimal polynomial $F \in L[t]$. Then $\Omega^1_{K/k}$ is the $K$-module given by $dx_1, \cdots, x_r, d\alpha$ subject to the single relation $F'(\alpha)d\alpha = 0$. (We're using 13.13 so get that $\Omega^1_{L/k} = \bigoplus_{i=1}^{r} L\ dx_i$.) Here we have $r + 1$ generators and 1 relation, and the thing $= 0$. So $r = 0$. ○

# LECTURE 18: NOVEMBER 14

The proof of 13.14 was wrong: we used the fact that the field extension was finite (i.e. finitely generated as a vector space), but the statement only said that it was finitely generated (i.e. finitely generated as a field). Interpolate the following lemma with proof of 13.14.

LEMMA 18.1. *(1) Suppose $K/k$ is a finite field extension and that $\overline{k}$ is an algebraic closure of $k$. Then $K/k$ is separable $\iff$ $K \otimes_k \overline{k}$ is reduced.*

*Proof.* Let $a \in K$ with minimal polynomial $f \in k[X]$. So $k[a] = k(a) \cong k[X]/(f)$ and $k \hookrightarrow k[a] \hookrightarrow K$. Over a field, every $k$-module is flat, so we get $\overline{k} \hookrightarrow k[a] \otimes_k \overline{k} \hookrightarrow K \otimes_k \overline{k}$ (i.e. these are actually subrings). Since $k(a) \cong k[X]/(f)$, we have that $k[a] \cong \overline{k}[X]/(f)$. Now $a$ is separable over $k$ iff $f$ has distinct roots in every field extension, in particular in $\overline{k}$. This happens iff $\overline{k}[X]/(f) \cong \overline{k} \oplus \cdots \oplus \overline{k}$ (by the Chinese remainder theorem: $f$ having distinct roots means that, when you factor $f$, you get coprime factors).

More precisely, over $\overline{k}$ we have

$$f = (X - \alpha_1)^{e_1} \cdot \cdots \cdot (X - \alpha_r)^{e_r}$$

with distinct $\alpha_i$, so

$$\overline{k}[X]/(f) \cong k[X]/(X^{e_1}) \oplus \cdots \oplus \overline{k}[X]/(X^{e_r})$$

Visibly $\overline{k}[X]/(f)$ is reduced, iff each $e_i = 1$, iff $f$ is separable, iff $a$ is separable over $k$. So $K \otimes_k \overline{k}$ is reduced, which implies $k[a] \otimes_k \overline{k}$ is reduced, which implies that $a$ is separable over $k$ for all $a$, or equivalently $K/k$ is separable. Conversely, suppose $K/k$ is separable. Then $K = k(a)$ for some $a$, and this is isomorphic to $k[X]/(f)$ with $f$ separable. The same argument shows that then $K \otimes_k \overline{k}$ is reduced. ○

LEMMA 18.2. *(2) Suppose $K/k$ is finite and algebraic. Then $K/k$ is separable iff $\Omega^1_{K/k} = 0$.*

*Proof.* $K/k$ is separable iff $K \otimes_k \overline{k}$ is reduced. Now $K = k[X_1, \cdots, X_n]/(f_1, \cdots, f_r)$. This implies that

$$\Omega^1_{K/k} = \bigoplus K \cdot dX_i/(df_j = 0 \ \forall j)$$

So for all $k \to R$, we see that $\Omega^1_{K \otimes_k R/R} = (\Omega^1_{K/k}) \otimes_k R$ (notice that $K \otimes_k R/R$ is a $K$-vector space), because $K \otimes_k R = R[X_1, \cdots, X_n]/(f_1, \cdots, f_r)$ (you don't change generators / relations, you just change coefficients).

Assume $\Omega^1_{K/k} = 0$. Take $R = \overline{k}$. So $\Omega^1_{K \otimes_k \overline{k}/\overline{k}} = 0$. Now $K \otimes_k \overline{k}$ is an Artinian ring (because it's finite-dimensional over $\overline{k}$, of dimension $[K : k]$), with all residue fields $\cong \overline{k}$ (by the Nullstellensatz). So $K \otimes_k \overline{k} = A_1 \oplus \cdots \oplus A_r$, each $A_i$ a local Artin $\overline{k}$-algebra, with residue field $\overline{k}$. Say $A_i = A$. So $(A, \mathfrak{m}, \overline{k})$ is Artin local, containing $\overline{k}$. Since $A$ is a quotient of $K \otimes_k \overline{k}$ we see that $\Omega^1_{A_i/\overline{k}} = 0$ (e.g. from the second fundamental exact sequence). So

there are maps

$$\begin{array}{ccccc} \overline{k} & \hookrightarrow & A & \twoheadrightarrow & \overline{k} \\ & & \downarrow & & \\ & & \mathfrak{m} & & \end{array}$$

So $A = \overline{k} \oplus \mathfrak{m}$. Then $A \twoheadrightarrow A/\mathfrak{m}^2 \xrightarrow{\cong} \overline{k} \oplus (\mathfrak{m}/\mathfrak{m}^2)$, where the multiplication on $\mathfrak{m}/\mathfrak{m}^2$ is zero. Assume $\mathfrak{m} \neq 0$, so $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ (by Nakayama). Pick any $\mathfrak{m}/\mathfrak{m}^2 \twoheadrightarrow \overline{k}$ (vector space surjection). This defines an algebra surjection

$$\overline{k} \oplus (\mathfrak{m}/\mathfrak{m}^2) \twoheadrightarrow \overline{k} \oplus \overline{k}\varepsilon = \overline{k}[t]/(\varepsilon^2)$$

$\Omega^1_{A/\overline{k}} = 0$ so then $\Omega^1_{\overline{k}[\varepsilon]/(\varepsilon^2)/\overline{k}} = 0$. But this is : $\Omega^1_{\overline{k}[\varepsilon]/(\varepsilon^2)} = \overline{k}[\varepsilon]d\varepsilon/(2\varepsilon \cdot d\varepsilon = 0)$ This has two generators, and you're killing one iff the characteristic is not 2. So it has $\overline{k}$-dimension (at least) one, and is nonzero as a $\overline{k}[\varepsilon]$-module.

So, we assumed $\Omega^1_{K/k} = 0$ and we've deduced that $K/k$ is separable.

Conversely, assume $K/k$ is separable, i.e. $K \otimes_k \overline{k}$ is reduced. Then our analysis via Artin rings shows that $K \otimes_k \overline{k} \cong \overline{k} \oplus \cdots \oplus \overline{k}$.

We want $\Omega^1_{K/k} = 0$. Well, $\Omega^1_{K/k} = 0 \iff \Omega^1_{K \otimes_k \overline{k}/\overline{k}} = 0$. (Field extensions, e.g. $k \to \overline{k}$, are faithfully flat: they are flat, and do not kill any module under $\otimes$.) To kill $\Omega^1_{K \otimes_k \overline{k}/\overline{k}}$, it is enough to show that every $\overline{k}$-derivation $D : K \otimes_k \overline{k} \to N$ is zero (i.e. in order to kill this module you just have to kill its dual). But $K \otimes_k \overline{k} = \overline{k} \oplus \cdots \oplus \overline{k}$, and it's easy to see that every $\overline{k}$-derivation of $\overline{k} \oplus \cdots \oplus \overline{k}$ is zero (calculate component by component). ○

Now return to the proof of 13.14 and observe that Lemmas 1 and 2 complete the proof.

Definition 18.3. Suppose $K/k$ is a field extension, finite-generated but not necessarily finite. A *separating transcendence basis* is a transcendence basis $(x_1, \cdots, x_r)$ of $K/k$ such that $K/k(x_1, \cdots, x_r)$ is separable. (An ordinary transcendence basis is a collection of algebraically independent elements $(y_1, \cdots, y_s)$ such that $K/k(y_1, \cdots, y_s)$ is algebraic.)

Proposition 18.4. *(13.16) Assume that $k$ is perfect and that $x_1, \cdots, x_r \in K$. Then $(x_1, \cdots, x_r)$ is a separating transcendence basis of $K/k$ iff $(dx_1, \cdots, dx_r)$ is a $K$-basis of $\Omega^1_{K/k}$.*

*Proof.* Assume $(dx_1, \cdots, dx_r)$ is a $K$-basis of $\Omega^1_{K/k}$. Put $L = k(x_1, \cdots, x_r)$ so there are inclusions $k \hookrightarrow L \hookrightarrow K$. We have an exact sequence

$$\Omega^1_{L/k} \otimes_L K \xrightarrow{u} \Omega^1_{K/k} \to \Omega^1_{K/L} \to 0$$

$\Omega^1_{L/k}$ is generated by $(dx_1, \cdots, dx_r)$, and $\Omega^1_{K/k}$ is based by the same things (i.e. the $dx_i$ generate *and* have no relations). So $u$ is an isomorphism, and $\Omega^1_{K/L} = 0$. Therefore, $K/L$ is algebraic and separable (Lemma 13.14). So suppose there is a polynomial relation of

minimal degree. We can write it as

$$\sum g_i(x_1, \cdots, x_{r-1}) x_r^i = 0$$

and not every $i \equiv 0 \pmod{p}$ (this is because $k$ is perfect). (If it were impossible, then every term that appears has an exponent divisible by $p$; every monomial would have a $p^{th}$ root, and every constant has a $p^{th}$ root, because $k$ is perfect.)

Let $M_1 = k(x_1, \cdots, x_{r-1})$. Then $L/M$ is algebraic. The exact sequence for differentials $\Omega^1$ shows that $\Omega^1_{L/M} \neq 0$, and $L/M$ is inseparable. This contradicts the fact that some $i$ is nonzero modulo $p$.

Converse: exercise. ○

# Lecture 19: November 16

Reminder: next 2 Saturdays – *lectures* at 2PM.

Let $K/k$ be a finitely generated field extension, where $k$ is perfect. We showed last time (Proposition 13.16) that some subset $(x_1, \cdots, x_r)$ is a separating transcendence basis iff $(dx_1, \cdots, dx_r)$ is a $K$-basis of $\Omega^1_{K/k}$.

Definition 19.1. Define $tr[K : k] := d$ if there exist $x_1, \cdots, x_d \in K$ such that

(1) $k(x_1, \cdots, x_d) \cong Frac(k[X_1, \cdots, X_d])$ (i.e. the $x_i$ are algebraically independent), and
(2) $K/k(x_1, \cdots, x_r)$ is algebraic and separable.

Corollary 19.2. *(13.17)* $tr[K : k]$ *is well-defined.*

*Proof.* $\dim_K \Omega^1_{K/k}$ is well-defined. ○

**Differentials and smoothness.** Assume $k$ is perfect (you lose very little if you assume $k$ is algebraically closed), and that $V$ is an affine algebraic variety over $k$. Suppose $p \in V$ is a closed point, i.e. $p$ corresponds to a maximal ideal $\mathfrak{m}_p$ of the coordinate ring $k[V]$. Put $K = k(p)/\mathfrak{m}_p$. The Nullstellensatz says that $K/k$ is a finite field extension. (If $k$ were algebraically closed, then the fields would be the same. But we want to think of $k$ as the field of definition, and $K$, which depends on the point.) Let $A = k[V]_{\mathfrak{m}_p} = \mathcal{O}_{V,p}$. If $\mathfrak{m}$ is the maximal ideal of $A$, then $K = A/\mathfrak{m}$.

A tangent vector to $V$ at $P$ is, by definition, a $k$-algebra homomorphism $A \to K[\varepsilon] := K[X(X^2)]$. Assume that

$$\begin{array}{ccc} A & \xrightarrow{v^{opp}} & K[\varepsilon] \\ \downarrow{\scriptstyle f_1} & \swarrow{\scriptstyle f_2} & \\ K = A/\mathfrak{m} & & \end{array}$$

is commutative, where $f_1$ is reduction modulo $\mathfrak{m}$, and $f_2$ is reduction modulo $\varepsilon$. Geometrically, this is a morphism

$$V \leftarrow \operatorname{Spec} K[e] \hookrightarrow \operatorname{Spec} K[x]$$

that factors as

$$\begin{array}{ccccc} V & \xleftarrow[v]{} & \operatorname{Spec} K[\varepsilon] & \hookrightarrow & \operatorname{Spec} K[x] \\ & & \uparrow & & \uparrow \\ \{p\} & \longleftarrow & \operatorname{Spec} K & & \\ \downarrow & \swarrow & & & \\ \operatorname{Spec} k & & & & \end{array}$$

where $\operatorname{Spec} K[x] = \mathbb{A}^1_K$, and $\operatorname{Spec} K[\varepsilon] \hookrightarrow \mathbb{A}^1_K$. I claim that $v$ is a tangent vector. In geometry, a tangent vector is an equivalence class of curves that go through your point at time 0, and are the same *to first order*. So That's what's going on here: mapping to $K[\varepsilon]$ is throwing away all the information beyond first order.

Given a morphism $A \to K = A/\mathfrak{m}$, how much information is required to construct $v^{opp}$? Answer: you nee a $K$-homomorphism $\mathfrak{m}/\mathfrak{m}^2 \to K \cdot \varepsilon$ (a 1-dimensional vector space). One 1-dimensional $K$-vector space is as good as any other, so you just need a $K$-homomorphism $A \to K$. So our tangent space *is* $(\mathfrak{m}/\mathfrak{m}^2)^\vee$. This is usually referred to as the Zariski tangent space to $V$ at the point $p$, denoted $T_pV = T_V(p)$. So $(\mathfrak{m}/\mathfrak{m}^2)$ is the *cotangent space*.

So at every closed point I have a tangent space and a cotangent space. The module of differentials is what ties together these things.

LEMMA 19.3. *(13.22) Define $\Omega^1_{V/k} := \Omega^1_{k[V]/k}$. There is a natural homomorphism*

$$\Omega^1_{V/k} \otimes_{k[V]} K(p) \xrightarrow{\cong} \mathfrak{m}_p/\mathfrak{m}_p^2$$

*(Recall $\Omega^1_{V/k} \otimes k[V] \cong \Omega^1_{V/k}/(\mathfrak{m}_p \cdot \Omega^1_{V/k})$.)*

*Proof.* We want a natural (i.e. basis-independent) isomorphism

$$T_pV \to \operatorname{Hom}_k \Omega^1_{V/k} \otimes_{k[V]} K, K \cdot \varepsilon$$

where the RHS is the module $\operatorname{Der}_k(k[V], (k[V]/\mathfrak{m}_p) \cdot \varepsilon)$ by the universal property of derivations. (A homomorphism $\Omega^1_{V/k} \to K \cdot \varepsilon$ kills the maximal ideal, so it's the same as a homomorphism $\Omega^1_{V/k} \otimes A/\mathfrak{m} \to K \cdot \varepsilon$. (If $I \cdot N = 0$ then $\operatorname{Hom}(M, N) = \operatorname{Hom}(M \otimes A/I, N)$.))

We know that $T_pV = \mathrm{Hom}\left(\mathfrak{m}_p/\mathfrak{m}_p^2 \to K\right)$. So it is enough to find a natural isomorphism

$$i : \mathrm{Hom}_{k-alg}(k[V]/\mathfrak{m}_p^2, K[\varepsilon]) \to \mathrm{Der}_k(k[V], K \cdot \varepsilon)$$

Suppose $\varphi \in LHS$. So $\varphi : k[]/\mathfrak{m}_p^2 \to K[\varepsilon]$. Define $i(\varphi)(a) = \mu\varepsilon$ if $\varphi(a \pmod{\mathfrak{m}_p^2}) = \lambda + \mu\varepsilon$. We need to produce an inverse for $i$. Given a $k$-derivation $D : k[V] \to K\varepsilon$ define $\varphi : k[V]/\mathfrak{m}_p^2 \to K[\varepsilon]$. Then

$$\varphi(a) = a \pmod{\mathfrak{m}_p} + D(a)$$

so we can define $i^{-1}$ by $i^{-1}(D) = \varphi$. ○

Suppose $V \hookrightarrow \mathbb{A}_k^n = \mathrm{Spec}\, k[X_1, \cdots, X_n]$ is defined by $f_1 = \cdots = f_r = 0$, and $\dim V = d$. Let $p \in V$ be a closed point.

Definition 19.4. $V$ is smooth at $p$ if the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$ (an $r \times n$ matrix with entries in $K(p)$) has rank $n - d$.

$J = \left(\frac{\partial f_i}{\partial x_j}\right)$ (the matrix of actual polynomials) appears in the exact sequence

$$\underbrace{I_V/I_V^2}_{\substack{\text{gen. by } \overline{f_1}, \cdots, \overline{f_r} \\ \overline{f_i} = f_i \pmod{I_v^2}}} \xrightarrow{J} \underbrace{\Omega^1_{\mathbb{A}/k} \otimes_{k[\mathbb{A}^n]}}_{\substack{\text{free } k[V]\text{-module} \\ \text{generated by } dx_1, \cdots, dx_n}} k[V] \to \Omega^1_{V/k} \to 0$$

where $J$ is the matrix w.r.t. the basis described. So $\Omega^1_{V/k} = \mathrm{coker}\, J$, so $\Omega^1_{V/k} \otimes_{k[V]} K \cong \mathrm{coker}\, J(p)$. The lower the rank of the Jacobian, the bigger the vector space $\mathrm{coker}\, J$.

One feature of this definition of smoothness is that $n - d$ is maximal. Why?

$$\Omega^1_{V/k} \otimes k[V]k(V) = \Omega^1_{k(V)/k} = k(V) - \text{vector spae of dim} = tr[k(V) : k] = \dim V$$

So $\Omega^1_{V/k}$ is a finitely-generated $k[V]$-module whose rank is exactly $\dim V$.

TBC tomorrow.

# Lecture 20: November 17

Let $k$ be a perfect field, $V \subset \mathbb{A}_k^n$ defined by $f_1, \cdots, f_r = 0$. So $k[V] = k[X_1, \cdots, X_n]/I$ where $I = (f_1, \cdots, f_n)$. Assume that $V$ is a variety, of dimension $d$. Look at the Jacobian matrix $J = \left(\frac{\partial f_i}{\partial x_j}\right)$. Pick a closed point $p \in V$; then we can evaluate $J(p) = \left(\frac{\partial f_i}{\partial x_j}(p)\right)$. $\mathrm{coker}\, J = \Omega^1_{V/k}$ in the sense that we have the second fundamental exact sequence

$$I/I^2 \to \Omega^1_{\mathbb{A}^n/k} \otimes_{k[\mathbb{A}^n]} k[V] \to \Omega^1_{V/k} \to 0$$

where the first homomorphism is "essentially" the Jacobian matrix. We say that $V$ is smooth at $p$ if $rank(J(p)) = n - d$.

DEFINITION 20.1. For any ring $A$ and finitely-generated $A$-module $M$ and prime ideal of $A$, $M$ is *free at $p$* iff $M_p$ is a free $A_p$-module.

PROPOSITION 20.2. *(13.23)*

(1) *$V$ (a variety of dimension $d$) is smooth at $P \iff$ the $k[V]$-module $\Omega^1_{V/k}$ is free at $p$. (Then its rank will be $d$.)*
(2) *The set of smooth points of $V$ is a Zariski-open subset of $V$.*

*Proof.* (1) $\Omega^1_{V/k}$ is generated by the $dx_j$'s, modulo the relations $df_i = 0$, where $df_i = \sum \frac{\partial f_i}{\partial x_j} dx_j$. So as we've seen, $\dim \Omega^1_{V_k} \otimes_{k[V]} K(p) = n - rank(J(p))$, as a $K(p)$-vector space (where $K(p) = k[V]/\mathfrak{m}_p$). The result follows from Lemma 13.24. ○

LEMMA 20.3. *(13.24) Suppose that $M$ is a finitely generated module over the Noetherian domain $A$. For any prime ideal $p$, $K(p) = Frac(A/p)$, or equivalently, $A_p/p_p$. Let $\eta = 0$ be the generic point, so $K(\eta) = Frac(A)$. Then*

(1) $\dim_{K(p)}(M \otimes_A K(p)) \geq \dim_{K(q)}(M \otimes_A K(q)) \geq \dim_{K(\eta)}(M \otimes_A K(\eta))$ *where $\eta \subset Q \subset P$.*
(2) *the set $P$ where the inequality is an equality, is Zariski-open in $A$.*

*Proof.* Suppose $rank(M) = r$. By definition, this is $\dim_{K(\eta)}(M \otimes_A K(\eta))$. Notice by Nakayama's lemma, $\dim_{K(p)}(M \otimes K(p))$ is the minimal number of generators of $M_p$, and $M \otimes K(p) = M_p/p \cdot M_p$.

Fix, once and for all, a presentation of $M$:

$$A^p \xrightarrow{\rho} A^q \xrightarrow{\pi} M \to 0$$

Now, take any $r$-tuple $(\widetilde{m}_1, \cdots, \widetilde{m}_r)$ of elements in $A^q$. This defines a homomorphism $A^r \xrightarrow{\sigma} A^q$. So $\rho + \sigma$ is a homomorphism $A^p \oplus A^r \to A^q$. This is a matrix, and you can compose with the map $A^q \to M$. $\rho + \sigma$ is surjective iff $\pi(\widetilde{m}_1), \cdots, \pi(\widetilde{m}_r)$ generate $M$. Let $m_i = \pi(\widetilde{m_i})$. Localize at $p$: $(\rho + \sigma)(p)$ is surjective iff $m_1, \cdots, m_r$ generate $M(p)$; i.e., the set of prime ideals $P$ where $m_1, \cdots, m_r$ fail to generate $M(p)$ is the cokernel of the matrix above, and hence is defined by the vanishing of a set of determinants, the maximal minors of the matrix $\rho + \sigma$.

So every $r$-tuple $(m_1, \cdots, m_r)$ of elements of $M$ gives a closed subset of prime ideals $P$ where the $m_i$ fail to generate $M(p)$. Take the intersection of all closed subsets over all $r$-tuples $(m_1, \cdots, m_r)$. This is the set of prime ideals $P$ at which $M$ cannot be generated by $r$ elements.

The key phrase is *Fitting ideal*.

(Moral: you can describe the singular locus in terms of matrices, hence in terms of determinants, which are polynomials, and so this is closed.)

(1) Lift generators of $M(p)$ to generators of $M$. If they generate $M(p)$, then by Nakayama they generate $M_p$, and hence generate $M_q$ where $q$ is a smaller prime. So those generators generate the module localized at the generic point. ○

We've started to prove things about affine varieties, but we really need to talk about projective varieties. Any smooth affine curve is gotten by deleting points out of a projective curve. Conversely, you can start with a projective curve and make an affine curve with deleting random points. But why would you do that? It's a destructive and arbitrary act.

EXAMPLE 20.4. Suppose $\dim V = 1$. A smooth curve $V$ has a sheaf $\Omega^1_{V/k}$. If $V$ is projective, $\Omega^1_{V/k}$ has a degree $2g-2$ where $g = \dim H^0(V, \Omega^1_{V/k})$ (the space of global sections). This is a finite-dimensional vector space over the field of definition. The point is that you can use differentials to get global invariants.

**Some aspects of homology.** This is mainly an issue of signs. We will talk about tensor products of chain complexes, and then the Koszul complex.

Suppose that $P = (\cdots \to P_n \to P_{n-1} \to \cdots)$ and $Q = (\cdots \to Q_n \to Q_{n-1} \to \cdots)$ are chain complexes of $A$-modules $P_i$ and $Q_i$.

LEMMA 20.5. *(16.1) Define $P \otimes_A Q$ as follows:*

- $(P \otimes Q)_n = \bigoplus_{i+j=n} P_i \otimes Q_j$
- *the differential is defined by*

$$d(p_i \otimes q_j) = dp_i \otimes q_j + (-1)^i p_i \otimes dq_j$$

(This sign is desired so that if $X, Y$ are cell complexes, then the cellular chain complex of $X \times Y$ is the tensor product of the cellular chain complexes of $X$ and $Y$.)

*Proof.* Check that $d^2 = 0$. ○

LEMMA 20.6. *(16.2) This tensor product is associative.*

*Proof.* Start by defining $P^1 \otimes \cdots \otimes P^r$ (with no parentheses). (The exponents indices of different complexes, not exponentiation.)

$$(P^1 \otimes \cdots \otimes P^r)_n = \bigoplus_{i_1+\cdots+i_r=n} (P^1_{i_1} \otimes \cdots \otimes P^r_{i_r})$$

(For notational convenience, omit the tensor symbol in products of elements.) Define the differential as

$$d(p_{i_1} \cdots p_{i_r}) = (dp_{i_1} \cdot p_{i_2} \cdots p_{i_r}) + (-1)^{i_1} p_{i_1} (dp_{i_2}) \cdot p_{i_3} \cdots p_{i_r} + \cdots + (-1)^{i_1+\cdots+i_{r-1}} p_{i_1} \cdots p_{i_{r-1}} (dp_{i_r})$$

(The sign is the sum of the degrees that $d$ has to cross before it operates.)

Then it is easy to define, e.g.

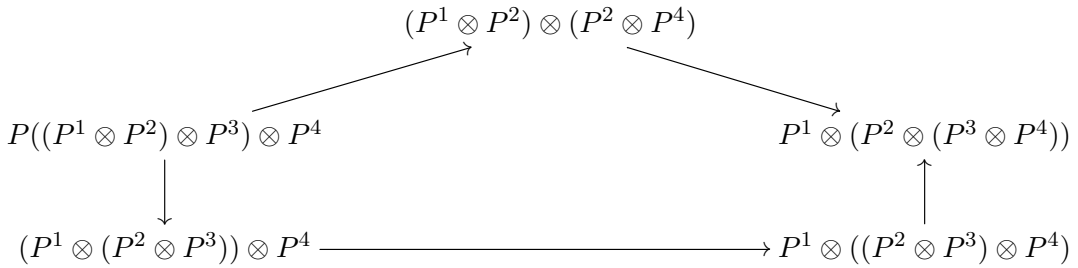
$$P^1 \otimes (P^2 \otimes P^3) \to P^1 \otimes P^2 \otimes P^3$$

by sending

$$p_i^1 \cdot (p_j^2 p_k^3) \mapsto p_i^1 p_j^2 p_k^3$$

(notation: $p_1^i$ is an element in the $i^{th}$ graded component of $P^1$, so the element on the left is in the $(i+j+k)$-graded piece of $P^1 \otimes (P^2 \otimes P^3)$). Conversely, there is an isomorphism $(P^1 \otimes P^2) \otimes P^3 \to P^1 \otimes P^2 \otimes P^3$. Using this and the analogous map for $(P^1 \otimes P^2) \otimes P^3$, get an isomorphism $\Phi_{123} : P^1 \otimes (P^2 \otimes P^3) \to (P^1 \otimes P^2) \otimes P^3$.

Then check the pentagon identity:




This is in Maclane's *Categories for the working mathematician*. Then all routes between two bracketed tensor products are equal.

Commutativity is less trivial.

○

# Lecture 21: November 19

Today, we will discuss commutativity.

Lemma 21.1 (Koszul sign rule). *(16.3) There is an isomorphism $\varphi : P \otimes Q \to Q \otimes P$ defined by*

$$\varphi(p_i \otimes q_i) = (-1)^{ij} q_j \otimes p_i$$

*where $p_i \in P_i$ and $q_j \in Q_j$.*

*Proof.* You need only check that $d\varphi = \varphi d$. ○

Consequence: if $P^1, \cdots, P^n$ and $g \in S_n$ is a permutation, there is an isomorphism

$$P^1 \otimes \cdots \otimes P^n \to P^{g(1)} \otimes \cdots \otimes P^{g(n)}$$

because any permutation $g$ can be written as a product of transpositions, where you interchange two adjacent letters. But, there are many ways of doing this, so there exist many isomorphisms.

QUESTION 21.2. Is there such an isomorphism that is functorial, not only in the complexes $P^1, \cdots, P^n$, but also under all embeddings $\{1, \cdots, n\} \hookrightarrow \{1, \cdots, n, n+1\}$?

The problem is one of signs, and the answer is "yes". The symmetric group, with the set of adjacent transformations, is a Coxeter system.

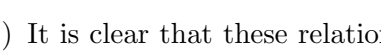
DEFINITION 21.3. A *Coxeter system* is a group $W$ and a finite subset $S = \{s_1, \cdots, s_r\} \subset W$ such that, for every pair $i, j = 1, \cdots, r$ there are $m_{ij} \in \mathbb{N} \cup \{\infty\}$ such that

(1) $W = \langle s_1, \cdots, s_r : (s_i s_j)^{m_{ij}} = 1 \ \forall i, j \rangle$
(2) $m_{ii} = 1$ (so every $s_i^2 = 1$)
(3) $m_{ij} \geq 2$ if $i \neq j$

DEFINITION 21.4. The associated *Dynkin diagram* is a graph with one vertex for each generator; the vertices $s_i$ and $s_j$ are disjoint if $m_{ij} = 2$ (equivalently $s_i s_j = s_j s_i$). They are joined by a blank edge if $m_{ij} = 3$, and are joined by an edge with $m_{ij}$ written above or beside it if $m_{ij} \geq 4$.

Note that $m_{ij} = \infty$ means that there is no relation.

EXAMPLE 21.5. If $W = S_n$, then $r = n - 1$, $s_i = (i, i+1)$, and the diagram is just



where there are $n - 1$ vertices. (This is type $A_{n-1}$.) It is clear that these relations hold, but you need to prove that these are a sufficient set of relations to define $S_n$.

PROPOSITION 21.6. *(16.4) Suppose $(W, S)$ is a Coxeter system whose Dynkin diagram is unlabelled. That is, $m_{ij} = 1, 2,$ or 3.*

*Suppose that $M$ is a representation of $W$ over a ring $R$ (i.e., I have an action of $W$ on $M$ as $R$-linear automorphisms), and suppose I have a map $f : S \to M$ of sets such that $S \cdot f(s) + f(s) = 0$ and the two "braid hypotheses" hold:*

(1) *$t \cdot f(s) + f(t) = s \cdot f(t) + f(s)$ is $s, t$ commute (i.e., the vertices are not joined)*
(2) *$st \cdot f(s) + s \cdot f(t) + f(s) = ts \cdot f(t) + t \cdot f(s) + f(t)$ (i.e. the vertices are joined by an edge; because we're not allowing edges with multiplicity, these two cases cover everything)*

*Observe: $s^1 = 1$ and $st = ts$ if the vertices are not joined, and $tst = sts$ if they are joined. (If you were allowing labelled edges, the relation would be $tstst \cdots = ststs \cdots$ (longer strings).)*

*Then*

(1) *$f$ extends uniquely to a map $f : W \to M$ that satisfies the constraint*
$$f(sg) = f(g) + g^{-1} f(s) \ \forall g \in W, s \in S$$
(2) *$f$ also satisfies*
$$f(hg) = f(g) + g^{-1} f(h) \ \forall g, h \in W$$

*Proof.* Idea: this is the standard kind of argument when you're proving theorems about Coxeter systems. This may not be of much help for you if you haven't worked with Coxeter systems. Proof in the next lecture. ○

COROLLARY 21.7. *(16.5) Take $W = S_n$, $S = \{s_j\}$, for $s_j = (j, j+1)$. Let $V = \bigoplus_{i=1}^n Re_i$ with its obvious permutation action. Let $M = \Lambda^2 V$ (a free $R$-module with basis $\{e_{pq} = e_p \wedge e_q : p < q\}$). Then:*

(1) *There is a unique map $f : S_n \to M$, where $f(s_j) = e_{j,j+1}$ and the braid hypotheses are satisfied.*
(2) *$f(g) = \sum e_p \wedge e_q$, where the sum is over all pairs $(p, q)$ such that $p < q$ and $g(p) > g(q)$.*

*Proof.* Must verify hypotheses of Proposition 16.4. Proof omitted. ("You just have to do it, and it's not particularly enlightening. The details teach you nothing, except that the result is true. Sometimes that's the way things are...") ○

PROPOSITION 21.8. *(16.6) Given complexes $P^1, \cdots, P^n$ and an element $g \in S_n$, there is an isomorphism*

$$\varphi_g : P^1 \otimes \cdots \otimes P^n \to P^{g(1)} \otimes \cdots \otimes P^{g(n)}$$

*such that $\varphi_{hg} = \varphi_h \circ \varphi_g$, and when $g = (j, j+1)$ then $\varphi_g$ is given by the Koszul sign.*

*These issues are functorial in the complexes and under enlarging $n$.*

*Proof.* Given $g \in S_n$, we want $\varphi_g$ to satisfy

$$\varphi_g(p^1_{i_1} \otimes \cdots \otimes p^n_{i_n}) = (-1)^{F(g;i_1,\cdots,i_n)} p^{g(1)}_{g(i_1)} \otimes \cdots \otimes p^{g(n)}_{g(i_n)}$$

where $F : S_n \times \mathbb{Z}^n \to \mathbb{Z}/2$ is a sign rule satisfying the constraints

$$\begin{aligned} F(hg; i_1, \cdots, i_n) &= F(h; i_{g(1)}, \cdots, i_{g(n)}) + F(g; i_1, \cdots, i_n) \\ F(s_j; i_1, \cdots, i_n) &= i_j i_{j+1} \\ F(1; i_1, \cdots, i_n) &= 0 \end{aligned}$$

Such an $F$ will give us the compatibilities we need. Fix indeterminants $x_1, \cdots, x_n$. Let $M$ be a $\mathbb{F}_2$-vector space spanned by monomials $x_i x_j$ for $1 \le i < j \le n$. $M$ is a space of quadratic polynomials $V \to \mathbb{F}_2$, where $V$ is the standard permutation representation of $S_n$ over $\mathbb{F}_2$.

Assume that $F(g, v) = f(g)(v)$, for some $f : S_n \to M$. Then, it is enough to construct $f : S_n \to M$ such that

$$\begin{aligned} f(s_j) &= x_j x_{j+1} \text{ (Koszul)} \\ f(hg)(v) &= f(h)(g(v)) + f(g)(v) \end{aligned}$$

(i.e. $f(hg) = g^{-1} f(h) + f(g)$). Now the existence of $f$ follows from Proposition 16.4.

Moreover, 16.5 gives

$$\varphi_g(p^1_{i_1} \otimes \cdots \otimes p^n_{i_n}) = (-1)^{\sum i_p i_q} p_{g(i_1)^{g(1)}} \otimes \cdots \otimes p^{g(n)}_{g(i_n)}$$

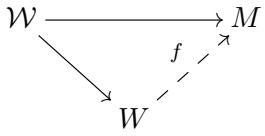
where the sum is taken over all pairs $(p, q)$ with $p < q$ and $g(p) > g(q)$. ○

I haven't told you everything, but at least I'm making clear what I'm not telling you. Matsumura just ignores the whole problem.

Exercise: Define $\varphi_g$ as above; then verify functoriality using the formula. (N.S.-B. says he couldn't do this. "The machinery of Coxeter groups exists; so use it.")

# Lecture 22: November 21

*Proof of Proposition 16.4.* Say $\mathcal{W}$ is the free group on $S$. We shall construct $F : \mathcal{W} \to M$, and then show that $F$ factors through $W$:




Let $\ell : \mathcal{W} \to \mathbb{N}$ is the length function: every element in $\mathcal{W}$ is a word in the elements of $S$, and $\ell$ counts the number of letters in the word. Note that $\ell(1) = 0$, $\ell(s^{\pm 1}) = 1$ for all $s \in S$. Define $F(1) = 0$, $F(s) = f(s)$, $F(s^{-1}) = f(s)$. Given $w \in \mathcal{W}$ with $\ell(w) > 1$, write $w = s^{\pm 1} \cdot w_1$, with $\ell(w_1) = \ell(w) - 1$. (Just pull off the first letter, which is either in $S$ or the inverse of something in $S$.) Assume inductively that $F(w_1)$ has been constructed. Then define

$$F(w) = F(w_1) + w_1^{-1} F(s) \tag{22.1}$$

Since $\mathcal{W}$ is free, this gives $F : \mathcal{W} \to M$. $M$ is a representation of $\mathcal{W}$. So $F$ satisfies property (1) of the desired extension.

Now show, by induction on $\ell(h)$, that

$$F(hg) = F(g) + g^{-1} F(h) \ \forall g, h \in \mathcal{W}$$

If $\ell(h) \leq 1$, then we're done by construction. If $\ell(h) \geq 2$, then $h = s^{\pm 1} h_1$, where $\ell(h_1) = \ell(h) - 1$, so that

$$F(hg) = G(s^{\pm 1} h_1 g) = g^{-1} h_1^{-1} F(s) + F(h_1, g)$$

by 220. By the induction hypothesis,

$$F(h, g) = g^{-1} F(h_1) + F(g)$$

So

$$\begin{aligned} F(hg) = F(s^{\pm 1} h_1 g) &= (h_1 g)^{-1} F(s^{\pm 1}) + F(h_1 g) \\ &= g^{-1} h_1^{-1} F(s^{\pm 1}) + \left( g^{-1}(h_1) + F(g) \right) \\ &= g^{-1} \left( h_1^{-1} F(s^{\pm}) + F(h_1) \right) + F(g) \\ &= g^{-1} F(h) + F(g) \end{aligned}$$

So our conclusions (1) and (2) hold for $(\mathcal{W}, F)$. We want to construct $f$. For this, it is enough to show that if $w_1, w_2 \in \mathcal{W}$ are equivalent (i.e. equal in $W$), then $F(w_1) = F(w_2)$.

We haven't used the Coxeter structure at all; every finitely-presented group can be written as a quotient of a free group. A basic result about Coxeter groups is this:

FACT 22.1. *Suppose we have a Coxeter group with no multiple edges. Given two equivalent words $w_1, w_2$, it is possible to pass from one to the other in a sequence $f$ elementary moves, each of which is one of:*

(1) *replace $sts$ with $tst$ if $s, t$ are joined;*
(2) *replace $st$ by $ts$ if $s, t$ are distinct and disjoint;*
(3) *replace $ss$ by 1 ("delete $ss$");*
(4) *replace an empty string 1 by the string $ss$ ("insert $ss$").*

*(1) and (2) are called the braid relations.*

Reference: http://www.math.ubc.ca/~cass/coxeter/crm1.html or Bourbaki, *Groupes et algèbres de Lie*, chapters IV - VI.

The point of Bourbaki is to get all the fundamentals out of the way so we can do something more interesting. This one is actually human-readable; it's self-contained and has all the foundational results.

It's easy to check that $F(sts) = F(tst)$, $F(st) = F(ts)$, and $F(ss) = F(1) = 0$ under appropriate circumstances. To prove $F(w_2) = F(w_1)$, we can assume that $w_2$ has been obtained from $w_1$ by exactly one of the moves (1) – (4), and that either (A) $w_1$ and $w_2$ begin with the same letter $s$, or (B) $w_1$ and $w_2$ end with the same letter $t$. (A single move is not enough to change the initial letter *and* the final letter, except for very short words (three letters or fewer), which we know how to deal with).

*Case (A):* $w_1 = su_1$ and $w_2 = su_2$, with $u_1$ and $u_2$ equivalent. (The move that takes $w_1$ to $w_2$ must be the move that takes $u_1$ to $u_2$.) By induction on length, $F(u_1) = F(u_2)$, and $F(w_1) = F(su_1) = F(u_1) + u_1^{-1}F(s) = F(u_2) + u_2^{-1}F(s) = F(w_2)$. Similarly, if $w_1 = v_1 t$ and $w_2 = v_2 t$. So $F : \mathcal{W} \to M$ induces $f : W \to M$, the uniqueness of $F$ gives the uniqueness of $f$, and (1) and (2) hold for $f$ because they hold for $F$.

The "fact" quoted above gives an algorithm for determining whether a word in a Coxeter group is trivial. This is unusual... in general the word problem is not solvable. ○

We applied this to $(W, S) = S_n$, and the generating set was the set of all transpositions, $\{(12), \cdots, (n-1, n)\}$. We deduced that the tensor product of complexes is commutative, with an explicit rule of signs.

EXERCISE/ RESEARCH PROBLEM 22.2. Find rules of signs for more general Coxeter systems, or find an interesting use for the rule we just discovered.

Actually, *don't* think about this.

EXAMPLE 22.3 (Koszul complex). Fix a ring $A$ and fix finitely many elements $x_1, \cdots, x_r$. (The most interesting situation is when $A$ is local, and the $x_i$'s are in the maximal ideal.) Write $X = (x_1, \cdots, x_n)$ (as a vector).

Define $K_\bullet = K_\bullet(X) = K_\bullet(x_1, \cdots, x_r)$, the Koszul complex associated to $A, X$ is defined by

$$\begin{aligned} K_0 &= A \\ K_1 = F_1 &= \bigoplus_{i=1}^{r} Ae_i \text{ free of rank } r \\ K_j &= \Lambda^j F_1, \quad \forall j = 0, \cdots, r \\ K_j &= 0 \ \forall j < 0, \quad \forall j > r \end{aligned}$$

So $K_j$ has a basis $e_{i_1} \wedge \cdots \wedge e_{i_j}$ for $i_1 < \cdots < i_j$. The differential $d : K_j \to K_{j-1}$ is defined by

$$d(e_{i_1} \wedge \cdots \wedge e_{ij}) = \sum_{m=1}^{j} (-1)^{m-1} x_{i_m} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_m}} \wedge \cdots \wedge e_{i_j}$$

Check that $d^2 = 0$, so $K_\bullet$ is a complex.

Homological algebra is never locally difficult; what's hard is maintaining the belief that you're doing something worthwhile.

# LECTURE 23: NOVEMBER 23

Last time we were talking about the Koszul complex. Take $x_1, \cdots, x_r \in A$, and denote $X = (x_1, \cdots, x_r)$ (a vector). We constructed the Koszul complex $K = K(X) = K(x_1, \cdots, x_r)$: this is a finite cochain complex

$$0 \to K_r \to \cdots \to K_1 \to K_0 = A \to 0$$

and each $K_j = \Lambda^j F_1$, where $F_1 = K_1 = \bigoplus_{i=1}^r Ae_i$ is a free module. The differential is

$$d(e_{i_1} \wedge \cdots \wedge e_{i_j}) = \sum_{m=1}^{j} (-1)^{m-1} x_{i_m} (e_{i_1} \wedge \cdots \wedge \widehat{e_{i_m}} \wedge \cdots \wedge e_{i_j})$$

For $x \in A$, $K(x)$ is isomorphic to the complex

$$\cdots \to 0 \to A \xrightarrow{x} A \to 0$$

where the nontrivial map is given by multiplication by $x$.

LEMMA 23.1. *(16.7)* $K(x_1, \cdots, x_r) \cong K(x_1) \otimes \cdots \otimes K(x_r)$

*Proof.* By induction on $r$. If $r = 1$ this is obvious. If $K = K(x_1, \cdots, x_{r-1})$ and $L = K(x_r)$, with $L_1 = Af$ (the free module with generator $f$), then $df = x_r$, and

$$(K \otimes L)_q = K_q \otimes L_0 \oplus K_{q-1} \otimes L_1$$

and

$$d(e_{i_1} \wedge \cdots \wedge e_{i_q} \otimes 1) = d(e_{i_1} \wedge \cdots \wedge e_{i_q}) \otimes 1$$
$$d(e_{i_1} \wedge \cdots \wedge e_{i_{q-1}} \otimes f) = d(e_{i_1} \wedge \cdots \wedge e_{i_{q-1}}) \otimes f + (-1)^{q-1} e_{i_1} \wedge \cdots \wedge e_{i_{q-1}} \otimes x_r$$

Identify $e_{i_q} \wedge \cdots \wedge e_{i_q} \otimes 1 = e_{i_1} \wedge \cdots \wedge e_{i_q}$ and $f = e_r$; then the result follows. ○

Since the tensor product of complexes is commutative, $K(X)$ is independent of the order of $x_1, \cdots, x_r$.

Suppose $M$ is a finitely-generated $A$-module. Regard $M$ as a complex concentrated in degree 0. Write $K(X; M) = K(X) \otimes M$. Define $H_p(X; M)$ to be the homology of this complex. (Call this the Koszul complex of $M$ wrt the elements $x_1, \cdots, x_r$.) Fix a single $x \in A$.

LEMMA 23.2. *(16.8) For any complex $L$ of $A$-modules, there is a short exact sequence*

$$0 \to H_0(K(x) \otimes H_p(L)) \to H_p(K(x) \otimes L) \to H_1(K(x) \otimes H_{p-1}(L)) \to 0$$

*$K(x)$ is a two-term complex, and so is $K(x) \otimes H_p(L)$ since $H_p(L)$ is a module.*

*Proof.* (Note that the first and third terms are both (homology of) two-term complexes.)

$$(K(x) \otimes L)_p = (K_0(x) \otimes L_p) \oplus (K_1(x) \otimes L_{p-1})$$

There is a short exact sequence of complexes

$$0 \to K_0(x) \otimes L \to K(x) \otimes L \to K_1(x) \otimes L[-1] \to 0$$

where the $[-1]$ means "shift to the right": the degree $p$ piece of $K_1(x) \otimes L[-1]$ is $K_1(x) \otimes L_{p-1}$; the degree $p$ piece of $K_0(x) \otimes L$ is $K_0(x) \otimes L_p$. A short exact sequence of chain complexes gives a long exact sequence in homology:

$$\begin{aligned}(23.1)\quad \cdots \to H_{p+1}(K_1(x) \otimes L[-1]) &\to H_p(K_0(x) \otimes L) \to H_p(K(x) \otimes L) \\ &\to H_p(K_1(x) \otimes L[-1]) \to H_{p-1}(K_0(x) \otimes L) \to \cdots\end{aligned}$$

Tensoring with a flat module (such as $K_1(x) = A = K_0(x)$) commutes with taking homology. So (23.1) is

$$\begin{aligned}(23.2)\quad \cdots &\to K_1(x) \otimes H_{p+1}(L[-1]) \to K_0(x) \otimes H_p(L) \to H_p(K(x) \otimes L) \\ &\to K_1(x) \otimes H_p(L[-1]) \to K_0(x) \otimes H_{p-1}(L) \to \cdots \\ &= \cdots \to \underbrace{K_1(x) \otimes H_p(L) \xrightarrow{\alpha} K_0(x) \otimes H_p(L)}_{K(x) \otimes H_p(L)} \to H_p(K(x) \otimes L) \\ &\qquad \to \underbrace{K_1(x) \otimes H_{p-1}(L) \xrightarrow{\beta} K_0(x) \otimes H_{p-1}(L)}_{K(x) \otimes H_{p-1}(L)} \to \cdots\end{aligned}$$

So we get a short exact sequence

$$0 \to \operatorname{coker} \alpha \to H_p(K(x) \otimes L) \to \ker \beta \to 0$$

$\alpha$ is $A \otimes H_p(L) \xrightarrow{x \otimes 1} A \otimes H_p(L)$, and so $\operatorname{coker} \alpha = H_p(L)/x \cdot H_p(L)$. But this is $(A/xA) \otimes H_p(L)$. This map is $K(x) \otimes H_p(L)$ and $\operatorname{coker} \alpha$ is $H_0$ of this. $\beta$ is multiplication by $x$ on $H_{p-1}(L)$, so $\ker \beta = H_1(K(x) \otimes H_{p-1}(L))$. ○

Corollary 23.3. *(16.9) If $M$ is an* acyclic complex *(that is, it's exact, except possibly in degree zero), $N = H_0(M)$ and $x$ is not a zero-divisor on $N$ then $K(x) \otimes M$ is acyclic and $H_0(K(x) \otimes M) = N/xN$.*

*Proof.* Take $M = L$ in Lemma 16.8. ○

Definition 23.4. Suppose $M$ is a module. The vector $X = (x_1, \cdots, x_m)$ is *$M$-regular* if each $x_i$ is not a zero-divisor on $M/(x_1, \cdots, x_{i-1})M$ for each $i$.

Proposition 23.5. *(16.11) If $X$ is $M$-regular, then $H_p(X; M) = 0$ for all $p \geq 1$.*

*Proof.* Assume inductively that $H_p(x_1, \cdots, x_{r-1}; M) = 0$ for all $p \geq 1$. Then the natural map

$$K_0(x_1, \cdots, x_{r-1}; M) \to H_0(x_1, \cdots, x_{r-1}; M) = M/(x_1, \cdots, x_{r-1})M$$

describes $K(x_1, \cdots, x_{r-1}; M)$ as an acyclic resolution of $M/(x_1, \cdots, x_{r-1})M$ and then Corollary 16.9 concludes. (Any acyclic complex $M$ is by definition an acyclic resolution of its $H_0$.) ○

Now assume $x_1, \cdots, x_r \in rad(A)$ (for example, if $A$ is local and all $x_i \in \mathfrak{m}$), and set $X = (x_1, \cdots, x_r)$.

Theorem 23.6. *(16.12) Fix a finitely-generated $A$-module $M$. T.F.A.E.:*

(1) $H_p(X; M) = 0 \ \forall p \geq 1$
(2) $H_1(X; M) = 0$
(3) *$X$ is $M$-regular.*

*Proof.* The only thing left is (2) $\implies$ (3): do this by induction. It's already done for $r = 1$. Put $Y = (x_1, \cdots, x_{r-1})$ and $z = x_r$. Assume the result for $K(Y; M)$. By Lemma 16.8, we have a short exact sequence

$$0 \to H_0(K(z) \otimes H_1(Y; M)) \to H_1(X; M) \to H_1(K(z) \otimes H_0(Y; M)) \to 0$$

We're assuming $H_1(X; M) = 0$, so both the submodule and the quotient are zero. $H_0 = 0$ implies that $H_1(Y; M) = z \cdot H_1(Y; M)$. By Nakayama's lemma, $H_1(Y; M) = 0$. (This only works because $z \in rad(A)$.) So $(x_1, \cdots, x_{r-1})$ is $M$-regular, by the induction hypothesis.

Since $H_1 = 0$, multiplication by $z$ is injective (i.e. $z$ is not a zero-divisor) in $H_0(Y; M) = M/(x_1, \cdots, x_{r-1})M$. ○

Corollary 23.7. *(16.13) If $x_1, \cdots, x_r \in rad(A)$, then the notion of $M$-regularity is independent of order.*

*Proof.* $K(X;M)$ is independent of the order. ○

REMARK 23.8. Suppose $(A,\mathfrak{m},k)$ is local [and $k \hookrightarrow A$] then if $(x_1,\cdots,x_r)$ is $A$-regular, then $r \leq \dim A$ [and the $x_i$ are algebraically independent]. The converse is false.

The rings that you can find a regular sequence of maximal length are called Cohen-Macaulay rings.

**Injective modules and injective resolutions.**

DEFINITION 23.9. An $A$-module $I$ is *injective* if, whenever you have an exact diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & N \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle g} & \\ & & I & & \end{array}$$

of solid arrows, there is a lifting $g$.

Injective objects are important in algebraic geometry, but projective objects (the dual) are very rare.

THEOREM 23.10. *Every $M$ can be embedded in an injective module.*

*Proof.* A series of lemmas.

LEMMA 23.11. *(17.2) A $\mathbb{Z}$-module is injective iff it is* divisible *(i.e. multiplication by $n$ is surjective for every $n$).*

REMARK 23.12. Standard examples are $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$.

*Proof.* Exercise. ○

LEMMA 23.13. *(17.3) Every $\mathbb{Z}$-module $G$ embeds in an injective $\mathbb{Z}$-module.*

*Proof.* Write $G = F/K$ where $F$ is free (there are many ways to do this). Then $F \cong \mathbb{Z}^{\oplus\alpha}$ (not necessarily finitely many factors), and there is an embedding

$$F \cong Z^{\oplus\alpha} \hookrightarrow \mathbb{Q}^{\oplus\alpha}$$

So there is an embedding

$$G \cong F/K \hookrightarrow \mathbb{Q}^{\oplus\alpha}/K,$$

which is divisible. ○

# LECTURE 24: NOVEMBER 24

The goal is to construct injective modules that contain a given module. We "know" that a $\mathbb{Z}$-module is injective iff it is divisible (e.g. $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}$); furthermore, every $\mathbb{Z}$-module embeds into an injective module.

Let $A$ be any commutative ring (this almost works in the non-commutative case, modulo replacing the ring by its opposite at certain points in the argument).

LEMMA 24.1. *(17.4) If $H$ is an injective $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(A, H)$ is an injective $A$-module.*

*Proof.* The $A$-module structure on $\mathrm{Hom}_{\mathbb{Z}}(A, H)$ is:

$$(a \cdot \varphi)(b) = \varphi(ab)$$

(This is dual to our other way of turning a $\mathbb{Z}$-module into an $A$-module: the tensor product.)

Suppose we are given

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\psi} & N \\ & & \downarrow{\scriptstyle f} & & \\ & & \mathrm{Hom}_{\mathbb{Z}}(A, H) & & \end{array}$$

Define $\varphi : M \to H$ by $\varphi(m) = f(m)(1)$. By the $\mathbb{Z}$-injectivity of $H$, $\varphi$ extends to a map $\theta : N \to H$. Define $g : N \to \mathrm{Hom}_{\mathbb{Z}}(A, H)$ by

$$g(n)(a) = \theta(an)$$

Verifying that $g(m) = f(m)$ is an exercise. ○

So there are lots of injective $A$-modules – for example, $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q})$.

LEMMA 24.2. *(17.5) Given an $A$-module $M$, there is an $A$-linear embedding $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, M)$.*

*Proof.* Define $\varphi(m)(a) = am$. ○

THEOREM 24.3. *(17.1) Given an $A$-module $M$, there exists an injective $A$-module $I$ and an embedding $A \hookrightarrow I$.*

*Proof.* There exists a $\mathbb{Z}$-linear embedding $M \hookrightarrow E$, where $E$ is an injective $\mathbb{Z}$-module. Also, $\mathrm{Hom}_{\mathbb{Z}}(A, E)$ is $A$-injective. Apply the functor $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ to $M \hookrightarrow E$ to get

$$\mathrm{Hom}_{Z}(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, E)$$

So $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, E)$ and $\mathrm{Hom}_{\mathbb{Z}}(A, E)$ is $A$-injective. ○

It follows that $M$ has an injective resolution. There is a long exact sequence

$$0 \to M \to I^0 \to I^1 \to \cdots$$

where $I^{i-1} \to I^i$ comes from embedding the cokernel of $I^{i-1} \to I^i$ for some injective object $I^i$ (and for $i = 1$, $I^0 \to I^1$ comes from embedding $I^0/M \hookrightarrow I^1$ for some injective $I^1$). That

is, there is an acyclic cochain complex

$$\mathcal{I} = I^\bullet = (\cdots \to 0 \to I^0 \to I^1 \to \cdots)$$

with $H^0(\mathcal{I}) = M$.

But there are many possible injective resolutions; the claim is that they're "closely related".

Definition 24.4. A *homomorphism of chain complexes* $M^\cdot \to N^\cdot$ is a collection of maps $M^n \to N^n$ that commute with the differential:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & M^n & \xrightarrow{d} & M^{n+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \\ \cdots & \longrightarrow & N^n & \xrightarrow{d} & N^{n+1} & \longrightarrow & \cdots \end{array}$$

Definition 24.5. Suppose $M^\bullet, N^\bullet$ are cochain complexes, and $f, g : M^\cdot \to N^\cdot$ are homomorphisms, then a *homotopy between $f$ and $g$* is a collection of homomorphisms $h : M^i \to N^{i-1}$ (where $h$ depends on $i$) such that

$$hd + dh = f - g$$

(Note that these are *not* cochain homomorphisms).

Lemma 24.6. *(17.6) If there is a homotopy between $f$ and $g$ then the homomorphisms $f^*, g^* : H^*(M) \to H^*(N)$ are equal.*

*Proof.* Exercise. ○

Lemma 24.7. *(17.7) Suppose $I, J$ are resolutions of $M$ (i.e. acyclic cochain complexes with first term $M$), and that $J$ is injective (i.e. every $J^n$ is injective).*

*Then there is a homomorphism $F : I \to J$ that extends $1_M$, and any two such homomorphisms are homotopic: i.e. if $G$ is another, then there is a homotopy between $F$ and $G$.*

*Proof.* Assume inductively that we've constructed

$$F^i : I^i \to J^i$$

for all $i \le r$. Define $Q^r := I^r / \operatorname{im} d$, and $R^r := J^r / \operatorname{im} d$. Then we have

$$\begin{array}{ccccc} 0 & \longrightarrow & Q^r & \longrightarrow & I^{r+1} \\ & & {\scriptstyle f^r}\downarrow & \overset{i \circ f^r}{\searrow} & \\ 0 & \longrightarrow & R^r & \xrightarrow[i]{} & J^{r+1} \end{array}$$

where $f^r = F^r$ modulo $\operatorname{im} d$. Take the composite $Q^r \to J^{r+1}$; the injective structure of $J^{r+1}$ guarantees that $i \circ f^r$ extends to $I^{r+1}$. So $F$ exists.

Homotopy: exercise. ○

COROLLARY 24.8. *(17.8) If $I$ and $J$ are injective resolutions of $M$ then there are homomorphisms $F : I \to J$ extending $1_M$ and $F' : J \to I$ extending $1_M$. So $F' \circ F : I \to I$ extends $1_M$ and $1_I : I \to I$ extends $1_M$. So, by part (2) of Lemma 17.7, there is a homotopy between $F' \circ F$ and $1_I$; similarly, there is a homotopy between $F \circ F'$ and $1_J$.*

Use this to define the right derived functors of any covariant left exact functor $\Phi$ from the category of $A$-modules to any other abelian category, for example the category of $B$-modules for some other ring $B$. For example, suppose $N$ is a fixed $A$-module. Take $\Phi = \mathrm{Hom}_A(N, -)$. (I'm particularly thinking of the category of quasicoherent sheaves over a scheme; all of the above and below basically carries over to this setting, so you can get injective resolutions and right derived functors.)

Recall, "left exact" means: if

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

is exact, then

$$0 \to \Phi(M') \to \Phi(M) \to \Phi(M'')$$

is exact. But if $M \twoheadrightarrow M''$ is surjective, applying a left exact functor $\Phi$ might well destroy surjectivity. If now

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

is exact, we will get a long exact sequence

$$\begin{aligned} 0 \to \Phi(M') \to \Phi(M) \to \Phi(M'') \\ \to R^1\Phi(M') \to R^1\Phi(M) \to R^1\Phi(M'') \\ \to R^2\Phi(M') \to R^2\Phi(M) \to R^2\Phi(M'') \end{aligned} \tag{24.1}$$

To construct/ define $R^i\Phi(M)$, take an injective resolution of $M$, say $I = (0 \to I^0 \to I^1 \to \cdots)$ (this is exact everywhere except in degree zero, where the cohomology is $M$ – think of it starting life as an exact sequence $0 \to M \to I^0 \to I^1 \to \cdots$). We get a complex

$$0 \to \Phi(I^0) \to \Phi(I^1) \to \cdots$$

Then define $R^i\Phi(M) = H^i(\Phi(I))$ (the $i^{th}$ cohomology of this complex).

We have to show that this is independent of the choice of injective resolution. Suppose $J$ is another injective resolution of $M$.

THEOREM 24.9. *(17.9) Our definition of $R^i\Phi(M)$ is independent of the choice of $I$.*

*Proof.* We have $F : I \to J$, $F' : J \to I$ such that both composites are homotopic to the identity: let $h : F' \circ F \to 1_I$ and $h' : F \circ F' \to 1_J$ be homotopies. Then

(1) $\Phi(h)$ is a homotopy from $\Phi(F') \circ \Phi(F)$ to $1_{\Phi(I)}$
(2) $\Phi(h')$ is a homotopy from $\Phi(F) \circ \Phi(F')$ to $1_{\Phi(J)}$.

Therefore, (1) implies that $\Phi(F') \circ \Phi(F)$ induces the identity on $H(\Phi(I))$, and in particular, on $H^i(\Phi(I))$ for every $i$. (2) implies that $\Phi(F) \circ \Phi(F')$ induces the identity on $H^i(\Phi(J))$ for every $i$. That is, the maps on $H^i$ induced by $\Phi(F)$ and $\Phi(F')$ are mutually inverse, i.e. they are isomorphisms. ○

We now know that right derived functors exist.

**Where does (24.1) come from?** We can construct injective resolutions $I, I', I''$ of $M, M', M''$ that are compatible, in these sense that we have a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^1 & \longrightarrow & I^1 & \longrightarrow & I''^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I'^2 & \longrightarrow & I^2 & \longrightarrow & I''^2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

such that the rows are exact. Apply $\Phi$ to get

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Phi(I'^0) & \longrightarrow & \Phi(I^0) & \longrightarrow & \Phi(I''^0) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

and the rows remain exact, because all the $I'$, $I$, $I''$ are injective (in particular, because $I'^i$ is injective). That is, we have a short exact sequence of complexes

$$0 \to \Phi(I') \to \Phi(I) \to \Phi(I'') \to 0$$

and such a thing always gives a long exact sequence of cohomology objects (easy exercise).

Lemma 24.10.

$$0 \to \Phi(I_1) \to \Phi(I_2) \to \Phi(I_3) \to 0$$

*is exact.*

*Proof.* Injectivity of $I_1$ gives a splitting of $0 \to I_1 \to I_2 \to I_3 \to 0$ via

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_1 & \longrightarrow & I_2 & \longrightarrow & I_3 & \longrightarrow & 0 \\
 & & {\scriptstyle Id}\downarrow & \swarrow & & & & & \\
 & & I_1 & & & & & &
\end{array}$$

○

Not every element of $M \otimes N$ is $m \otimes n$. For example, $M^p, N^q$ are finite-dimensional vector spaces over $k$. Then

$$\{m \otimes n\} \hookrightarrow M \otimes N = \mathbb{A}^{pq}$$

is the Segre embedding of

$$\mathbb{P}(M) \times \mathbb{P}(N) = \mathbb{P}^{p-1} \times \mathbb{P}^{q-1} \hookrightarrow \mathbb{P}^{pq-1}$$

where $\mathbb{P}(M)$ is the set of lines in $M$.

- *Primary ideal* $I$: if $xy \in I$ then $x \in I$ or $y \in \sqrt{I}$ (5.1)