Course notes for Modern Algebra

Instructor: Paul Smith
Scribe: Avi Levy

June 6, 2014

These are my notes for Math 506, taught by Paul Smith at the UW in Spring 2014. They are updated online at:

http://www.math.washington.edu/~avius

Contents

Math 506 Modern Algebra Notes by Avi Levy

Lecture 1: March 31

Affine Algebraic Geometry

The Zariski topology on $k^n = \mathbb{A}^n_k$ (affine n-space) takes the closed sets to be

$$V(f_1, f_2, \cdots) = \{p \in \mathbb{A}^n \mid f_1(p) = f_2(p) = \cdots = 0\}$$

where $f_1, f_2, \cdots \in k[x_1, \cdots, x_n]$ (viewed as k-valued functions on k^n). We'll check it's a topology in due course.

For any set A, let

$$V(A) = \{p \in \mathbb{A}^n \mid f(p) = 0 \ \forall f \in A\}.$$

Note. $V(f_1, f_2, \cdots) = V(I)$ where I is the ideal $(f_1, f_2, \cdots)$.

Proof. The easy direction is $V(f_1, f_2, \cdots) \supset V(I)$ (because $p \in V(I) \Rightarrow f_1, \cdots \in I$ all vanish). The reverse inclusion $V(I) \supset V(f_1, \cdots)$ holds since if $f_1(p) = f_2(p) = \cdots = 0$, then $(f_1 g_1 + \cdots + f_m g_m)(p) = 0$ for all $g_1, \cdots \in k[x]$. □

We will soon see that the polynomial ring $k[x_1, \cdots, x_n]$ is Noetherian. Then from the last result, $V(f_1, f_2, \cdots) = V(f_1, \cdots, f_r)$ for some finite subset.

Proposition 1.1. *Let I, J and $I_\lambda, \lambda \in A$, be ideals in $A = k[x_1, \cdots, x_n]$. Then*

1. $I \subset J \implies V(I) \supset V(J)$
2. $V(0) = \mathbb{A}^n$
3. $V(A) = V(1) = \varnothing$
4. $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$
5. $V(I) \cup V(J) = V(IJ) = V(I \cap J)$

Hence the Zariski Topology is in fact a topology.

Proof. The first three are obvious.

4. If $p \in \cap V(I_\lambda)$ and $f = \sum_{\text{finite}, \lambda \in \Lambda} f_\lambda$ where $f_\lambda \in I_\lambda$, then

$$f(p) = \sum f_\lambda(p) = 0$$

whence $\bigcap_\lambda V(I_\lambda) \subset V(\sum_\lambda I_\lambda)$. Conversely, if $p \in V(\sum I_\lambda)$ then $p \in V(I_\lambda)$ by (1).

5. Since $IJ \subset I \cap J$, we have $V(IJ) \supset V(I \cap J)$ and since $I \cap J \subset I$, also $V(I) \subset V(I \cap J)$. Likewise for J, so
$$V(IJ) \supset V(I \cap J) \supset V(I) \cup V(U).$$
Also if $p \notin V(I) \cup V(U)$, then there is an $f \in I$ and $g \in J$ such that $f(p) \neq 0$ and $g(p) \neq 0$. Hence the product $(fg)(p) = f(p)g(p) \neq 0$. Since $fg \in IJ$, it follows that $p \notin V(IJ)$. Hence $V(IJ) \subset V(I) \cup V(J)$.

□

Example 1.2. A subset of $\mathbb{A}^1_k$ (affine line over k) is closed if and only if it is $\mathbb{A}^1$ or $V(f)$ for some $0 \neq f \in k[x]$ (since $\mathbb{A}^1_k$ is principal). Conversely, given a finite subset of $\mathbb{A}^1$ we can form a polynomial with roots at those points. Thus the Zariski topology is the finite complement topology in this case.

Proposition 1.3. *If $f \in k[x_1, \cdots, x_n]$, then the function $f: \mathbb{A}^n_k \to k$ is continuous (in fact, the Zariski topology is minimal with respect to this property).*

Proof. We have to show that the preimage of a closed set is closed. But $f^{-1}\{\lambda\} = V(f - \lambda)$, so by taking finite unions we are done. □

From now on, the topology is always the Zariski topology.

Definition 1.4. Let $X \subset \mathbb{A}^n$ be any subset. Define
$$I(X) = \{f \in k[x_1, \cdots, x_n] \mid f(p) = 0 \ \forall p \in X\}$$

Lemma 1.5. $V(I(X)) = \overline{X}$

In particular when X is closed, $V(I(X)) = \overline{X}$.

Proof. First $I(X)$ is an ideal:

(a) $0 \in I(X)$

(b) If $f, g \in I(X)$ so is $f \pm g$ because
$$f(p) = g(p) = 0 \Rightarrow (f \pm g)(p) = 0$$

(c) If $f \in I(X)$ and g is any polynomial and $p \in X$, then $(fg)(p) = f(p)g(p)$ whence $fg \in I(X)$.

It is clear that $X \subset V(I(X))$. Taking closures yields $\overline{X} \subset V(I(X))$.

For the other direction, write $\overline{X} = V(J)$ for some ideal J. Then every function in J vanishes on every point of X, so $J \subset I(X)$. Since V is order-reversing, $V(J) \supset V(I(X))$. Thus $\overline{X} \supset V(I(X))$. Combined with the last paragraph, we see $\overline{X} = V(I(X))$. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 2: April 2

Hilbert's Basis Theorem

In this quarter, all rings are commutative with identity.

Theorem 2.1. *If R is a noetherian ring so is the polynomial ring $R[x]$.*

Proof. If $R[x]$ is not noetherian, then it would have an infinitely generated ideal I. Choose $f_1 \in I$ with minimal degree. Given $f_1, \cdots, f_i$, choose $f_{i+1} \in I \setminus (f_1, \cdots, f_i)$ with minimal degree. Note this process doesn't terminate.

Let a_i be the leading term of f_i. Since A is noetherian, the chain of ideals

$$(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, a_2, \cdots, a_n) \subset \cdots$$

stablizes. Thus $(a_1, \cdots) = (a_1, \cdots, a_m)$. Consequently $a_{m+1} = \sum_{j=1}^{m} r_j a_j$. Set

$$g = \sum_{j=1}^{m} r_j f_j x^{d_{m+1} - d_j}, \qquad \text{where } d_i = \deg f_i.$$

It follows that $\deg(f_{m+1} - g) < \deg f_{m+1}$, since the leading terms cancel. Now f_{m+1} has minimal degree in $I \setminus (f_1, \cdots, f_m)$. Thus $f_{m+1} - g \in (f_1, \cdots, f_m)$, and consequently $f_{m+1} \in (f_1, \cdots, f_m)$. This contradicts our construction; hence $R[x]$ admits no infinitely-generated ideals. Thus it is noetherian.

Note: The proof we did in class is slightly different. □

Corollary 2.2. $k[x_1, \cdots, x_n]$ *is noetherian.*

Definition 2.3. If $A \subset R$ are commutative rings, an element $b \in B$ is **integral over** A if it satisfies a monic polynomial with coefficients in A, i.e.

$$b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 = 0,$$

for some $a_{n-1}, \cdots, a_0 \in A$.

We say that B is **integral over** A if every element of B is integral over A.

Theorem 2.4 (Noether Normalization)**.** *Let $R = k[a_1, \cdots, a_n]$ be a finitely generated commutative k-algebra. Then there exists $C = k[y_1, \cdots, y_m]$ a polynomial ring with $m \leq n$ such that $C \subset R$ and R is integral over C.*

Example 2.5. Take $B = k[x, x^{-1}]$, and $A = k[x + x^{-1}]$. Then

$$x^2 - (x + x^{-1})x + 1 = 0,$$

so x is integral over A. Similarly, x^{-1} is integral. Thus by a theorem we're going to prove, $k[x, x^{-1}]$ is integral over A.

Proposition 2.6. *Let $R \subset S$ be rings and $\alpha \in S$. The following are equivalent:*

1. *α is integral over R*
2. *$R[\alpha]$ is a finitely generated R-module*
3. *There is a ring R' such that $R \subset R' \subset S$ and $\alpha \in R'$, with R' a finitely generated R-module.*

Recall that $R[\alpha]$ is the smallest subring of S containing R and α.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 3: April 4

Lemma 3.1. $R \subset S$, $a \in S$. *The following are equivalent:*

1. a *is integral over* R
2. $R[a]$ *is a finitely generated* R*-module*
3. *There is a ring* S' *such that* $R[a] \subset S' \subset S$ *and* S' *is a finitely generated* R*-module*

Proof. (1) $\Rightarrow$ (2). If $a^n + r_{n-1}a^{n-1} + \cdots + r_1 a + r_0 = 0$ for some $r_i \in R$, then $a^n \in R + Ra + \cdots + Ra^{n-1}$. Hence $R[a] = R + Ra + \cdots + Ra^{n-1}$.

(2) $\Rightarrow$ (3). Take $S' = R[a]$.

(3) $\Rightarrow$ (1) is the hard part. Write $S' = \sum_{i=1}^{n} Rs_i$ where each $s_i \in S'$, and (without loss of generality) $s_1 = 1$ (we can always throw it in). Since $a \in S'$, as is s_i, we have $as_i \in S'$ and hence $as_i = \sum_{j=1}^{n} \lambda_{ij} s_j$ with $\lambda_{ij} \in R$. Then $\sum_{j=1}^{n} (a\delta_{ij} - \lambda_{ij}) s_j = 0$. Let M be the $n \times n$ matrix with $M_{ij} = a\delta_{ij} - \lambda_{ij}$. Then

$$M \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0.$$

Take M' to be the adjugate matrix (i.e., transpose of the cofactors). Then $M'M \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \det(M) \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0$. But $s_1 = 1$, so $\det(M) = 0$. Now $\det(M) = a^n + \mathrm{l.d.t.}$, whereupon a is integral over R. □

Corollary 3.2. *Let* $R \subset S$ *be rings and* $a, \cdots, a_n \in S$. *If all the* a_i*'s are integral over* R*, then* $R[a_1, \cdots, a_n]$ *is a finitely generated* R*-module, hence integral over* R.

Proof. "fg R" means "finitely generated R-module".

Induct on n. By the lemma, $R[a_1]$ is fg R. Hence if $b \in R[a_1]$, then $R[b] \subset R[a]$ so by (3) $\Rightarrow$ (1), b is integral over R. This handles the $n = 1$ case.

Suppose that $R[a_1, \cdots, a_{n-1}]$ is fg R. Then $R[a_1, \cdots, a_{n-1}] = \sum_{i=1}^{k} Rs_i$. By (1) $\Rightarrow$ (2), we have $R[a_n]$ is also fg R, say $R[a_n] = \sum_{j=1}^{m} Rt_j$. Without loss of generality, assume $s_1 = t_1 = 1$ (need it for the identity element in the ring we're about to construct). Now $\sum_{i=1}^{n} \sum_{j=1}^{m} Rs_i t_j$ is fg R and also a ring. Lastly, by double inclusion it is $R[a_1, \cdots, a_n]$. By (3) $\Rightarrow$ (1) with $S' = R[a_1, \cdots, a_n]$, every element of $R[a_1, \cdots, a_n]$ is integral over R. □

Corollary 3.3. *If* $R \subset S$ *and* $a, b \in S$ *are integral over* R*, then* $a + b$ *and* ab *are integral over* R.

Proof. Apply the previous corollary to $R[a, b] \subset S$. □

Corollary 3.4. *Let* $R \subset S$. *Then*

$$\{a \in S \mid a \text{ is integral over } R\}$$

is a subring of S.

Theorem 3.5. *Let* R *be a domain,* $T \supset R$ *a domain that is integral over* R. *Then* R *is a field if and only if* T *is a field.*

- $\Rightarrow$ Let $a \in T \setminus \{0\}$. Then $a^n + r_{n-1}a^{n-1} + \cdots + r_1 a + r_0 = 0$ for some $r_i \in R$. Pick the smallest n that works. Then $r_0 \neq 0$ so $a(a^{n-1} + r_{n-1}a^{n-2} + \cdots + r_2 a + r_1) = -r_0$. Hence T is a field.
- $\Leftarrow$ Let $b \in R \setminus \{0\}$. Then $b^{-1} \in T$, so it satisfies a polynomial $b^{-n} + r_{n-1}b^{-n+1} + \cdots + r_1 b^{-1} + r_0 = 0$. Consequently $b^{n-1} + r_{n-1} + \cdots + r_1 b^{n-2} + r_0 b^{n-1} = 0$, so $b^{-1} \in R$.

Theorem 3.6. *Let* k *be a field and* $R = k[a_1, \cdots, a_n]$ *be a ring. Then there are* $y_1, \cdots, y_m \in R$, $m \leq n$, *such that*

1. *the* y_i*'s are algebraically independent*
2. R *is integral voer* $k[y_1, \cdots, y_m]$
3. R *is fg* $k[y_1, \cdots, y_m]$.

Proof. (Nagata)

$R = k[x_1, \cdots, x_n]/I$ for some polynomial ring and some ideal I. If $I = 0$, then we're done. Assume $I \neq 0$ and induct on n. The case $n = 1$ is clear.

We will produce a subring $T \subset R$ that is generated by $n - 1$ elements and R is integral over T. Then by applying the induction hypothesis,

$$S = k[y_1, \cdots, y_{m \leq n-1}] \subset T \subset R$$

with T integral over the polynomial ring S and R integral T. Thus T is fg S by corollary 1, and R is fg T by the same result. Now

$$\begin{aligned} R &= \sum_{j=1}^{p} T r_j \\ &= \sum_{j=1}^{p} \sum_{i=1}^{q} S t_i r_j, \end{aligned}$$

so R is fg S and hence integral over S. Next time we will produce the ring T. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 4: April 7

Theorem 4.1 (Noether Normalization)**.** *Let* k *be a field, and* $R = k[a_1, \cdots, a_n]$*. Then there is an* $m \leq n$ *and algebraically independent* $y_1, \cdots, y_m \in R$ *such that* R *is integral over* $k[y_i]$*.*

Nagata. $n = 0$ easy, $n = 1$ easy. Now we induct.

First, assume $k[a_i]$ is integral over $k[y_i]$ up to s with $s \leq n-1$ and y_i alg. indep. Then $k[y_i]$ in $k[a_i]$ up to $n-1$ adjoin a_n (inclusion is integral)

Write $R = k[x_1, \cdots, x_n]/I$. If $I = 0$, done. Suppose $I \neq 0$. Pick $0 \neq f \in I$ then $f(a_i) = 0$. Let $r_2, \cdots, r_n \in \mathbb{N}$ and define $z_2 = a_2 - a_1^{r_2}, z_3 = a_3 = a_1^{r_3}, \cdots, z_n$. Now $R = k[z_2, \cdots, z_n][a_1]$. If a_1 is intregral over $k[z_i]$ we're don by induction because $k[t_2, \cdots, t_q] \subset k[z_2, \cdots, z_2] \subset R$ and each inclusion is integral, $q <= n-1$

Notice that the polynomial

$$g(X) = f(X, z_2 + X^{r_2}, \cdots, z_n + X^{r_n})$$

vanishes at $X = a_1$. This $g(X)$ is a polynomial in X with coefficients in $k[z_2, \cdots, z_n]$. Will pick r_i so that g becomes monic. If the term $\alpha x_1^{i_1} \cdots x_n^{i_n}$ appears in f, then $g(X)$ has a term like

$$\alpha X^{i_1 + i_2 r_2 + \cdots + i_n r_n} + \mathrm{ldt}$$

Choose

$$N > \max\{i_j \mid x_j^{i_j} \text{appears somewhere in } f.\}.$$

Set $r_2 = N, r_3 = N^2, \cdots, r_n = N^{n-1}$ so all the high degree terms in $g(X)$ are different and can't cancel (due to base N representation). Then the leading term of $g(X)$ has coefficient in k. Thus without loss of generality, $g(X) \in k[z_2, \cdots, z_n][X]$ has leading term X^h for some h. Since $g(a_1) = 0$, it follows that a_i is integral over $k[z_2, \cdots, z_n]$. □

Corollary 4.2. *Let* k *be a field and* $K = k[x_1, \cdots, x_n]/I$ *another field. Then* $\dim_k K < \infty$*.*

Proof. By Noether normalization, K is integral over $k[y_1, \cdots, y_m]$ a polynomial ring with $m \leq n$. We already saw that an integral extension $R \subset S$ implies R is a field if and only if S is a field. Consequently $k[y_1, \cdots, y_m]$ is a field, i.e. $m = 0$. Thus K is integral over k.

Observe that $K = k[a_1, \cdots, a_n]$ (the images of the x_i). Starting with k, keep appending; then we get K finite dimensional over k. □

Theorem 4.3 (Hilbert's (weak) Nullstellensatz)**.** *If* k *is algebraically closed, then every maximal ideal in* $k[x_1, \cdots, x_n]$ *is of the form* $(x - \alpha_1, \cdots, x_n - \alpha_n)$ *for some* $(\alpha_1, \cdots, \alpha_n)$*.*

Proof. Uses Noether normalization. If $\mathfrak{m}$ is a maximal ideal of $k[x_1, \cdots, x_n]$ then $k[x_1, \cdots, x_n]/\mathfrak{m}$ is a field. In addition, it is finitely generated as a k-algebra, so by the corollary it has finite k-dimension. Since k is algebraically closed, it must be k itself. It follows that $x_i - \alpha_i \in \mathfrak{m}$

for some $\alpha_i \in k$ (since its a 1d vector space, x_i and 1 are linearly dependent). Hence $(x_1 - \alpha_1, \cdots, x_n - \alpha_n) \subset \mathfrak{m}$, and the reverse inclusion happens for dimension reasons (?). The result follows. □

Lemma 4.4. *Let* I *be an ideal in a ring* R*. If* R *is noetherian, then* I *contains a product of prime ideals.*

Proof. Let A be the set of ideals J that do not contain a product of prime ideals, and suppose A is non-empty. By the noetherian condition, there is a maximal element $J \in A$. Then J is not prime, since $J \supset J^2$. Hence, there are ideals I_1, I_2 such that $I_1, I_2 \notin J$ yet $J \supset I_1 I_2$. Hence $J \supset (J + I_1)(J + I_2)$ and both are strictly bigger than J, so not in A. Then J contains a product of primes, contradiction. □

Definition 4.5. Let J be an ideal in R. The **radical** of J is

$$\sqrt{J} = \{x \in R \mid x^n \in J\} \qquad \text{for some } n$$

Lemma 4.6. $\sqrt{J}$ *is an ideal*

Proof. If $x \in \sqrt{J}$ and $r \in R$, then $(xr)^n = x^n r^n \in J$ for some large n. If $x, y \in \sqrt{J}$ then $x^n, y^n \in J$ for some large n so by binomial theorem, $(x + y)^{2n} \in J$. □

Definition 4.7. An ideal I is called **radical** if $I = \sqrt{I}$.

Definition 4.8. If p is a prime ideal and $I \subset p$, we say p is **minimal over** I if the only prime q satisfying $I \subset q \subset p$ is $q = p$.

Proposition 4.9. *Let* I *be an ideal in a noetherian ring* R*.*

1. I *has finitely many minimal primes* p_k
2. $\bigcap p_k = \sqrt{I}$ *and* $\prod p_k^{i_k} \subset I$ *for some integers* $i_k > 0$.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 5: April 9

Graded Rings

A $\mathbb{Z}$-graded ring is a ring R together with a decomposition

$$R = \oplus_{n\in\mathbb{Z}} R_n$$

where each R_n is an abelian group and $R_i R_j \subset R_{i+j}$. You can do this with other abelian groups than just $\mathbb{Z}$. The standard example is $R = k[x_1, \cdots, x_t]$. Here $R_0 = k$, $R_1 = kx_1 + \cdots + x_t$, and $R_n = (R_1)^n = \text{span}\{x_1^{i_1} \cdots x_t^{i_t} \mid i_1 + \cdots + i_t = n\}$. The elements in R_n are called **homogeneous of degree** n.

An ideal I in R is **graded** if $I = \oplus_{n\in\mathbb{Z}}(I \cap R_n)$.

Lemma 5.1. *I is graded if and only if I is generated by homogeneous elements.*

Note. If $a \in R_n$, then aR is a graded ideal because $aR = aR_0 \oplus aR_1 \oplus \cdots$.

Exercise: If I, J are graded ideals, so are $I + J$, $I \cap J$, IJ, $\sqrt{I}$.

Definition 5.2. A **graded module** is an R-module M endowed with a decomposition $M = \oplus_{n\in\mathbb{Z}} M_n$ into abelian groups such that $R_i M_j \subset M_{i+j}$ for all i, j.

Pause for a second and say that 0 has degree $-\infty$, to avoid issues in that last statement. If M is a graded module and $N \subset M$ is a graded submodule ($N = \oplus(N \cap M_n)$), then M/N is a graded module with $(M/N)_n = (M_n + N)/N$.

Examples:

1. As an example take $k[x]$ with $\deg(x) = 1$ (it could be something else, no problem). Then (x^n) is a graded ideal and $(x^n)/(x^{n+m})$ is a graded module.

2. $D = \mathbb{C}[t, \partial]$. Set $\deg(\partial) = -1$ and $\deg(t) = 1$. Then $\mathbb{C}[t]$ becomes a graded left D-module with $\mathbb{C}[t]_n = \mathbb{C}t^n$. (One really starts with the natural grading on the polynomial ring, and that induces the grading on D)

   We only need the relation $\partial t - t\partial = 1$, which is homogeneous. Thus $\mathbb{C}\langle x, y\rangle/(xy - yx - 1)$ becomes a graded object, and in fact gives rise to our example.

3. $\mathbb{C}[x, y]/(y^2 - x^3)$ is graded, with $\deg(x) = 2$ and $\deg(y) = 3$. Then $\deg(x^i y^j) = 2i + 3j$. Then $y^2 - x^3$ is homogeneous of degree 6 so we may pass to the quotient and impose a grading. The moral is that we need not always give our indeterminates the standard grading of 1, and other situations are also natural. For instance, send $x \to t^2$ and $y \to t^3$.

Remark: When dealing with k-algebras, we almost always insist that all homogeneous components of k-vector spaces are k-subspaces. Thus we don't tend to make $\mathbb{C}$ a $\mathbb{Z}/2$ graded ring with $\deg(\mathbb{R}) = 0$ and $\deg(\mathbb{R}i) = 1$. The exception is "supermathematics", the mathematics of supersymmetry.

Now we state a general principle, as a lemma.

Lemma 5.3. *If* $f\colon R \to S$ *is a homomorphism between graded rings such that* $f(R_n) \subset S_n$ *for all* n*, then* $\operatorname{Ker} f$ *is a graded ideal and* $\operatorname{Im} f$ *is a graded subalgebra.*

Definition 5.4. Let R be a graded ring. The **category of graded R-modules** is called $\mathrm{Gr}(R)$. Its objects are the graded R-modules, and its morphisms are the degree-preserving R-module homomorphisms; this means $f\colon M \to N$ with $f(M_i) \subset N_i$ for all i.

$\mathrm{Gr}(R)$ is an Abelian category , but we won't say what that means.

Definition 5.5. For $M \in \mathrm{Gr}(R)$, let $M(n) \in \mathrm{Gr}(R)$ denote M with the same R-module structure but with the grading $M(n)_i = M_{n+i}$. The functor $F_n\colon \mathrm{Gr}(R) \to \mathrm{Gr}(R)$ given by $M \mapsto M(n)$ is called the **degree shift functor**.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 6: April 11

Graded Vector Spaces

Definition 6.1. A vector space V has a **good grading** if $V = \oplus_{n\in\mathbb{Z}} V_n$, $\dim V_n < \infty$ for all n, and $V_n = 0$ for large negative n.

For such a V, the **Hilbert series** is

$$H(V;t) = \sum_{n\in\mathbb{Z}} (\dim V_n) t^n.$$

The Hilbert series is a formal power series, used to encode the dimension data.

If U, V are vector spaces with good gradings, then

$$U \otimes V = \bigoplus_{i+j=n} U_i \otimes V_j,$$

which is a good grading on $U \otimes V$.

Remark. If U, V are vector spaces with bases u_i, v_j then $u_i \otimes v_j$ is a basis for $U \otimes V$. In particular, $\dim(U \otimes V) = (\dim U)(\dim V)$.

This allows us to compute $H(U \otimes V; t)$:

$$\begin{aligned} H(U \otimes V; t) &= \sum_{n\in\mathbb{Z}} \sum_{i+j=n} \dim(U_i)\dim(V_j) t^{i+j} \\ &= \left(\sum_{i\in\mathbb{Z}} (\dim U_i) t^i\right)\left(\sum_{j\in\mathbb{Z}} (\dim V_j) t^j\right) \\ &= H(U;t)H(V;t). \end{aligned}$$

The last summation makes sense because we have a good grading (so there are no issues for large negative i, j).

Remark. Useful facts about the tensor product:

1. For elements of $R \otimes S$, we have $(r \otimes s)(r' \otimes s') = (rr') \otimes (ss')$
2. $k[x] \otimes k[y] \simeq k[x, y]$
3. $R \otimes k[y] \simeq R[y]$

Proposition 6.2. *Consider* $k[x_1, \cdots, x_n]$ *with grading* $\deg(x_i) = q_i > 0$. *Then*

$$H(k[x_1, \cdots, x_n]; t) = \frac{1}{1-t^{q_1}} \frac{1}{1-t^{q_2}} \cdots \frac{1}{1-t^{q_n}}$$

Proof. $k[x_1, \cdots, x_n] = k[x_1] \otimes \cdots \otimes k[x_n]$, so

$$H(k[x_1, \cdots, x_n]; t) = \prod_{m=1}^{n} H(k[x_m]; t) = \prod_{m=1}^{n} \frac{1}{1 - t^{q_m}}.$$

□

We may apply these techniques to solve a homework problem.

Example 6.3 (Problem 3, Homework 1)**.** Consider $\phi : \mathbb{C}[x, y] \to \mathbb{C}[z^2, z^3]$ given by $x \mapsto z^2$ and $y \mapsto z^3$. Let $K = \ker \phi$ and $I = (x^3 - y^2)$. Then $K = I$.

Proof. Give $\mathbb{C}[x, y]$ the grading $\deg x = 2, \deg y = 3$, and give $\mathbb{C}[z]$ the grading $\deg z = 1$. Since

$$0 \to K \to \mathbb{C}[x, y] \to \mathbb{C}[z^2, z^3] \to 0$$

is exact, we obtain

$$\begin{aligned} H(K; t) &= H(\mathbb{C}[x, y]; t) - H(\mathbb{C}[z^2, z^3]) \\ &= \frac{1}{(1 - t^2)(1 - t^3)} - \frac{1}{1 - t} + t. \end{aligned}$$

We are adding in the missing term in degree 1. Meanwhile,

$$\begin{aligned} H(I; t) &= t^6 H(\mathbb{C}[x, y]; t) \\ &= \frac{t^6}{(1 - t^2)(1 - t^3)} \\ &= \frac{1}{(1 - t^2)(1 - t^3)} - \frac{1}{1 - t} + t \\ &= H(K; t). \end{aligned}$$

It's easy to see that $I \subset K$; thus by a dimension count, we have verified that $I = K$. □

Invariant Theory (i.e., Death and Resurrection)

Definition 6.4. Given a ring R and an action of G on R, its **ring of invariants** is

$$R^G = \{f \in R \mid g(f) = f \ \forall g \in G\}$$

Let G be a finite subgroup of $GL(n, k)$. Observe that $kx_1 \oplus \cdots \oplus kx_n \simeq k^n$. Thus we may think of $kx_1 \oplus \cdots \oplus kx_n$ as n-tuples, and define an action by

$$G \to \mathrm{Aut}_k(k[x_1, \cdots, x_n]), \qquad x \mapsto g.x = g(x), \qquad x \in kx_1 \oplus \cdots \oplus kx_n.$$

Big problem from 1800-1900: determine $k[x_1, \cdots, x_n]^G$. For example, S_n acts on $k[x_1, \cdots, x_n]$ by permutations ($\sigma : x_i \mapsto x_{\sigma(i)}$)

Theorem 6.5 (Newton)**.**

$$[x_1, \cdots, x_n]^{S_n} = k[u_1, \cdots, u_n],$$

where

$$\begin{aligned} u_1 &= x_1 + \cdots + x_n \\ u_2 &= x_1^2 + \cdots + x_n^2 \\ &\vdots \\ u_k &= x_1^k + \cdots + x_n^k \end{aligned}$$

In this case, there are no relations between the u_i; but we can think of other examples where this is not the case.

Example 6.6. 1. $\mathbb{Z}_n = \langle \sigma \rangle$ acting on $\mathbb{C}[x, y]$ as follows:

$$\sigma(x) = \xi x, \qquad \sigma(y) = \xi^{-1} y, \qquad \xi = e^{2\pi i/n}.$$

2. Then $\mathbb{C}[x^n, xy, y^n] = \mathbb{C}[x, y]^{\mathbb{Z}_n}$, and the first is $\simeq \frac{\mathbb{C}[x_0, x_1, x_2]}{(x_0 x_2 - x_1^n)}$. For many years people were working hard on this problem, calculating away to show finite generation of these rings; this is a non-trivial question, because there are plenty of infinitely generated subrings of $\mathbb{C}[x_1, \cdots, x_n]$.

Hilbert killed off this field by using abstract methods; people were upset. He did it using a grading, because things are homogeneous.

Proposition 6.7. *Let $S = S_0 \oplus S_1 \oplus \cdots$ be a (commutative) $\mathbb{N}$-graded k-algebra, and $R \subset S$ a graded subalgebra. Suppose there is a graded R-submodule $M \subset S$ such that $S = R \oplus M$. If S is a finitely generated k-algebra, then so is R.*

An indication of how this proposition solves the problem:

Theorem 6.8. *For a ring k of characteristic 0, let $S = k[x_1, \cdots, x_n]$ and G be a finite group of degree-preserving automorphisms of S. In other words, if $\sigma \in G$ then $\sigma(S_d) \subset S_d$ for all d. Then S^G is a finitely generated k-algebra.*

Before the theorem of Hilbert, finding the invariants was not known to be a finite process. Once you've got this, you are a quotient of a polynomial ring and hence you are Noetherian. Then there are only a finite number of relations.

Proof. To prove it, go back to the representation theory of G. Since characteristic is 0 and the group is finite, kG is semisimple (last quarter). Let $V_0, \cdots, V_t$ be the irreducible representations of G. Without loss of generality, V_0 is the trivial representation. Define $S(0), \cdots, S(t)$ by $S(j) = \sum$ of all simple G-submodules of S that are isomorphic to V_j.

Obviously, $S = S(0) \oplus \cdots \oplus S(t)$, and $S(0) = S^G$. This is because the ring of invariants consists of those polynomials such that $\sigma(f) = f$. In that case, kf is a 1-dimensional representation of G in which every element acts as the identity.

Notice that each $S(j)$ is an $S(0)$-module. To see why, let $f \in S(0)$. The map

$$\phi : S \to S, \qquad \phi(a) = fa$$

is a kG-module homomorphism, since if $\sigma \in G$ then

$$\phi(\sigma(a)) = f\sigma(a) = \sigma(f)\sigma(a) = \sigma(fa) = \sigma(\phi(a)$$

(since σ is an automorphism). Hence $\sigma\phi = \phi\sigma$, and ϕ is a kG-module homorphism.

Consequently, $\phi(S(j)) \subset S(j)$ for all j. To see why, take a simple submodule that is isomorphic to $S(j)$. The image of under ϕ is either 0 or isomorphic to V_j. Thus all the simple sobmodules isomorphic to V_j get sent to simple submodules that are isomorphic to V_j and the result follows.

It follows that $S(j)$ is an $S(0)$-module, whereupon $S = S^G \oplus (S(1) \oplus \cdots \oplus S(t))$. Now the proposition implies that S^G is a finitely generated k-algebra. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 7: April 14

We need this proposition to finish up the proof from last time about rings of invariants.

Proposition 7.1. *Let $S = k \oplus S_1 \oplus \cdots$ be a graded k-algebra, $R \subset S$ a graded subalgebra, and $M \subset S$ an R-graded submodule of S such that $S = R \oplus M$. If S is a finitely generated k-algebra, then so is R.*

Proof. Let $\mathfrak{m} = R_1 \oplus R_2 \oplus \cdots$ be a graded maximal ideal of R. Since S is finitely generated, S is noetherian. Thus $S\mathfrak{m} = a_1 S + \cdots + a_t S$ for some $a_i \in \mathfrak{m}$. We may suppose that each a_i is homogeneous. We claim that the finitely generated k-algebra $T = k[a_1, \cdots, a_t]$ is equal to R.

Suppose $T \subsetneq R$. Pick $f \in R \setminus T$ homogeneous and of minimal degree. Since $k \subset T$, $\deg f > 0$. Hence $f \in \mathfrak{m}$, which means

$$f = a_1 b_1 + \cdots + a_t b_t,$$

where the b_i are homogeneous.

The projection map $\pi : S \to R$ given by $\pi(r \oplus \mathfrak{m}) = r$ is a graded R-module homomorphism. Thus

$$f = \pi(f) = a_1 \pi(b_1) + \cdots + a_t \pi(b_t).$$

But $\deg(b_j) = \deg(f) - \deg(a_j) < \deg f$. Hence $\deg(\pi(b_j)) \leq \deg(b_j) < \deg f$. Hence by minimality, $\pi(b_j) \in T$. As a result, $f \in T$. So we've shown $T = R$, as desired. □

Now we embark on another (more geometric) way to think about gradings.

Remark. If S is a graded $\mathbb{C}$-algebra, then define $\varphi : \mathbb{C}^\times \to \mathrm{Aut}_{\mathbb{C}} S$. Then

$$\varphi(\xi)\left(\sum_{s_i \in S_i} s_i\right) = \sum \xi^i s_i.$$

Conversely if $\mathbb{C}^\times$ acts as automorphisms on S in a "reasonable" way, then S is a graded $\mathbb{C}$-algebra with

$$S_n = \{s \in S \mid \xi \cdot s = \xi^n s\}.$$

This can be interpreted in terms of symmetries of varieties.

Proposition 7.2 (Our goal)**.** $I(V(J)) = \sqrt{J}$

To get there, we will need the Strong Nullstellensatz.

Lemma 7.3. $V(J) = V(\sqrt{J})$

Proof. Since $J \subset \sqrt{J}$ and V is order-reversing, $V(\sqrt{J}) \subset V(J)$ is immediate.

Let $p \in V(J)$. If $f \in \sqrt{J}$, then $f^n \in J$ for some n, so

$$0 = f^n(p) = (f(p))^n.$$

Since the base field k has no nilpotents, it follows that $f(p) = 0$. Thus $V(J) \subset V(\sqrt{J})$ and the result follows. □

Theorem 7.4 (Hilbert's Strong Nullstellensatz)**.** $k = \overline{k}$ *and* $A = k[x_1, \cdots, x_n]$.

1. *If* $J \neq A$ *is an ideal, then* $V(J) \neq \varnothing$.
2. *For every ideal* $J \in A$, $I(V(J)) = \sqrt{J}$ *and* $V(I(X)) = \overline{X}$.
3. *There is bijection between closed varieties of* $\mathbb{A}^n (\simeq k^n)$ *and radical ideals in* A, *given by* $X \mapsto I(X)$ *and* $V(J) \hookleftarrow J$.

This is the "perfect bijection" that breathes life into algebraic geometry.

Proof. 1. follows from the weak Nullstellensatz, because $J \subset m = (x_1 - \alpha_1, \cdots, x_n - \alpha_n)$ for some $(\alpha_1, \cdots, \alpha_n) \in k^n$.

2. $\sqrt{J} \subset I(V(J))$ and $V(\sqrt{J}) = V(J)$, so it remains to show that if f vanishes on $V(J)$ then $f^r \in J$ for some $r > 0$.

   Sneaky trick: let $f \in I(V(J))$, and consider y a new indeterminate. Consider the ideal $(fy - 1, J)$ in $k[x_1, \cdots, x_n, y]$. A point $(\alpha_1, \cdots, \alpha_n, \beta)$ belongs to $V(fy - 1, J)$ if and only if $(\alpha_1, \cdots, \alpha_n) \in V(J)$ and $f(\alpha_1, \cdots, \alpha_n)\beta = 1$.

   Since $f \in I(V(J))$, if $(\alpha_1, \cdots \alpha_n) \in V(J)$ then $f(\alpha_1, \cdots, \alpha_n) = 0$. Consequently $f(fy - 1, J) \neq \varnothing$. It follows by (1) (i.e., the weak Nullstellensatz) that $(fy - 1, J) = k[x_1, \cdots, x_n, y]$. Hence

   $$1 = (fy - 1)h_0 + \sum_{i=1}^{m} g_i h_i$$

   where $J = (g_1, \cdots, g_m) \subset k[x_1, \cdots, x_n]$ and $h_i \in k[x_1, \cdots, x_n, y]$.

   Define $\Psi : k[x_1, \cdots, x_n, y] \to k(x_1, \cdots, x_n)$ (i.e. $\operatorname{Frac} k[x_1, \cdots, x_n]$). By setting $\Psi(x_i) = x_i$ and $\Psi(y) = \frac{1}{f}$. Then every element in $\operatorname{Im}(\psi)$ is of the form af^{-d} for some $a \in k[x_1, \cdots, x_n]$ and $d \geq 0$. Now

   $$\begin{aligned} 1 &= \Psi(1) \\ &= \Psi\left((fy - 1)h_0 + \sum_{i=1}^{m} g_i h_i\right) \\ &= \sum_{i=1}^{m} g_i \psi(h_i). \end{aligned}$$

Thus $1 = \sum_{i=1}^{m} g_i a_i f^{-d_i}$, $d_i \geq 0$ and $a_i \in k[x_1, \cdots, x_n]$. Hence for large enough D, we have

$$f^D = \sum g_i a_i f^{D-d_i} \in J.$$

The strong Nullstellensatz follows.

□

Proposition 7.5. *Every ideal in a noetherian ring contains a product of prime ideals.*

Lemma 7.6. *If p is a prime ideal containing J, then p contains $\sqrt{J}$.*

Proof. If $f \in \sqrt{J}$, then $f^n \in J$ for some $n > 0$. Thus $f^n \in p$, so by primality $f \in p$. □

The picture to keep in mind is $0 \subset J \subset \sqrt{J} \subset p \subset R$ (thought of as points lying one over the other).

Lemma 7.7. *If p is a prime containing J and $p_1^{e_1} \cdots p_n^{e_n} \subset J$, then some p_i is contained in p.*

Lemma 7.8. *If J is an ideal in a noetherian ring such that $J \supset p_1^{e_1} \cdots p_n^{e_n}$ for some primes p_i, then without loss of generality we can assume that each $p_i \supset \sqrt{J}$.*

Proof. The zero ideal in R/J contains a product of primes. A standard argument completes the proof (think intuitively). □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 8: April 16

Proposition 8.1. *Let I be an ideal in a noetherian ring. Then there are finitely many minimal primes over I and integers $i_k > 0$ such that $p_1^{i_1} \cdots p_r^{i_r} \subset I$.*

Proof. We have already seen that the 0 ideal in R/I contains a product of primes. They are the images of prime ideals in R that contain I. The result follows. □

Proposition 8.2. *There is a unique decomposition such that for distinct i, j,*

$$p_i \not\subset p_j \qquad (\star)$$

Proof. Start with any decomposition as before. If $p_k \supset p_j$ then we can replace $p_k^{i_k}$ by $p_j^{i_k}$. Thus there exists a decomposition that satisfies $(\star)$.

If there is a prime q such that $p_k \supset q \supset I$, then $\prod p_k^{i_k} \subset I \subset q$. Hence for some i, $p_i \subset q \subset p_k$. Thus $p_i = q = p_k$, so each p_k is a minimal prime over I.

Moreover, every minimal prime over I appears among the $\{p_i\}$ because if q is minimal, then $\prod p_k^{i_k} \subset q$. Then some $p_k \subset q$, so minimality of q implies that $p_k = q$. □

Let X be a closed subvariety of $\mathbb{A}_k^n$ where $k = \bar{k}$. Define

$$\mathcal{O}(X) = \frac{k[x_1, \cdots, x_n]}{I(X)}$$

Then $f \in \mathcal{O}(X)$ is a well-defined function $f : X \to k$.

Definition 8.3. $\mathcal{O}(X)$ is called **the ring of regular functions** on X.

Proposition 8.4. *The Zariski topology on $\mathbb{A}^n$ restricts to a topology on X.*

Proof. There is a bijection

$$\{\text{closed subsets of } X\} \leftrightarrow \{\text{radical ideals in } \mathcal{O}(X)\};$$

it is an immediate consequence of the analogous bijection for $\mathbb{A}^n$. □

Let X be a topological space.

Definition 8.5. X is **noetherian** if every chain of closed subspaces of X

$$X_1 \supset X_2 \supset \cdots$$

stabilizes.

Corollary 8.6. *$\mathbb{A}^n$ with the Zariski topology is noetherian.*

Proof. Such a descending chain corresponds to an ascending chain

$$I(X_1) \subset I(X_2) \subset \cdots$$

in the noetherian ring $k[x_1, \cdots, x_n]$. Since the chain stabilizes, we obtain $I(X_m) = I(X_{m+1})$. Then

$$X_m = V(I(X_m)) = V(I(X_{m+1})) = X_{m+1}.$$

□

Definition 8.7. A closed subset of a topological space X is **irreducible** if it s not a union of two proper closed subspaces.

Example 8.8. The ideal (xy) corresponds to the union of the axes and is reducible.

Proposition 8.9. *Let X be a noetherian topological space. Then there is a unique decomposition*

$$X = X_1 \cup \cdots \cup X_n \qquad (\star)$$

where each X_i is a closed irreducible subspace of X and $X_i \not\subset X_j$ and $X_j \not\subset X_i$ when $i \neq j$.

Proof. First, we show existence. Suppose that X cannot be decomposed like $(\star)$. Then $X = Y_1 \cup Z_1$ where Y_1, Z_1 are closed and non-empty, and one of them cannot be written in this form; say Y_1 cannot be decomposed like $(\star)$. Continuing inductively, we may write $Y_k = Y_{k+1} \cup Z_{k+1}$ to obtain a chain

$$X \supset Y_1 \supset \cdots \supset Y_n \supset \cdots$$

Now X is noetherian, so the chain stabilizes. This $Y_k = Y_{k+1}$, which is a contradiction. Hence $X = X_1 \cup \cdots \cup X_n$ is a finite union of irreducible subspaces.

Given a decomposition $X = X_1 \cup \cdots \cup X_n$, we can assume without loss of generality that $X_i \not\subset X_j$ and $X_j \not\subset X_i$ when $i \neq j$.

Now for uniqueness. If $X = Y_1 \cup \cdots Y_m$ where each Y_j is irreducible, then

$$\begin{aligned} X_1 &= X_1 \cap (Y_1 \cup \cdots \cup Y_m) \\ &= (X_1 \cap Y_1) \cup \cdots \cup (X_1 \cap Y_m). \end{aligned}$$

Since X_1 is irreducible, it follows that $X_1 = X_1 \cap Y_i$ for some i; hence $X_1 \subset Y_i$. By symmetry, $Y_j \subset X_j$ for some j. Thus $X_1 \subset X_j$ so $X_1 = Y_i$. Hence

$$\{X_1, \cdots, X_n\} \subset \{Y_1, \cdots, Y_m\}.$$

By symmetry, the reverse inclusion follows, and with it uniqueness. □

Proposition 8.10. *Let $X \subset \mathbb{A}^n$ be a closed subvariety. Then*

$$\{X \textit{ is irreducible}\} \Leftrightarrow \{I(X) \textit{ ix prime}\}$$

Proof. $\Rightarrow$ Suppose $fg \in I(X)$. If $p \in X$, then $0 = (fg)(p) = f(p)g(p)$ so either $f(p) = 0$ or $g(p) = 0$. Hence

$$X \subset V(f, I(X)) \cup V(g, I(X))$$

and

$$V(f, I(X)) \subset V(I(X)) = \overline{X} = X.$$

Thus $X = V(f, I(X)) \cup V(g, I(X))$. But X is irreducible so one of sets in the union is X. But if $V(f, I(X)) = X$, then $f \in I(X)$.

$\Leftarrow$ Suppose $X = Y \cup Z$ with Y, Z closed and $Z \neq X$. The bijection in the strong nullstellensatz tells us that $I(Z) \supsetneq I(X)$. Pick $f \in I(Z) \setminus I(X)$, $g \in I(Y)$, and $p \in X$.

Either $f(p) = 0$ or $g(p) = 0$. Thus $(fg)(p) = 0$, so $fg \in I(X)$. Now $I(X)$ is prime and $f \notin I(X)$, so $g \in I(X)$. Consequently $I(Y) \subset I(X)$, i.e. $X \subset Y$ and therefore $X = Y$.

□

Math 506 Modern Algebra Notes by Avi Levy

Lecture 9: April 18

Irreducible Components

Proposition 9.1. *Let R be a noetherian ring, I and ideal and $p_1, \cdots, p_r$ the minimal primes over I. Then*

$$\sqrt{I} = p_1 \cap \cdot \cap p_r.$$

Proof. We know that $p_1^{i_1} \cdots p_r^{i_r} \subset I$ for some integers $i_k > 0$. Then $(p_1 \cdots p_r)^k \subset I$ for some large k. Hence $(p_1 \cap \cdots \cap p_r)^{kr} \subset I$, so $p_1 \cap \cdots p_r \subset \sqrt{I}$.

For the other direction, notice that every prime over I contains $\sqrt{I}$ (Lemma 7.6). Thus $\sqrt{I} \subset p_1 \cap \cdots \cap p_r$. □

Theorem 9.2. *Let $X \subset \mathbb{A}^n$ be a closed subset. The irreducible components of X are $V(p_1), \cdots, V(p_r)$ where $p_1, \cdots, p_r$ are the minimal primes over $I(X)$.*

Proof. Since $I(X)$ is a radical ideal (by the Strong Nullstellensatz), $I(X) = p_1 \cap \cdots \cap p_r$. Therefore

$$\begin{aligned} X &= V(I(X)) \\ &= V(p_1 \cap \cdots \cap p_r) \\ &= V(p_1) \cup \cdots \cup V(p_r) \qquad (\star). \end{aligned}$$

Last time, we saw that $V(p_1)$ is irrediculble. If $i \neq j$, then $p_i \not\subset p_j$ and $p_j \not\subset p_i$. Hence $V(p_i) \not\subset V(p_j)$ and $V(p_j) \not\subset V(p_i)$. Thus $(\star)$ is the decomposition of X into its irreducible components. □

For many purposes, one can study an algebraic variety X by studying its individual irreducible components. Many results in commutative algebra start with the hypothesis that the ring is a domain. This is a sensible thing to do, in light of the irreducible decomposition. It's like assuming a manifold is connected.

The Spectrum

Definition 9.3. If R is a commutative ring, its **spectrum** is

$$\operatorname{Spec} R = \{\text{all primes ideals in } R\}.$$

This set is given the **Zariski topology** by declaring the closed sets to be of the form

$$V(I) = \{p \in \operatorname{Spec} R \mid p \supset I\}$$

for ideals $I \subset R$.

Lemma 9.4 (This is a topology)**.** *1.* $V(0) = \operatorname{Spec} R$

2. $V(R) = \varnothing$

3.
$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$$

4.
$$\bigcup_{\text{finite}} V(I_j) = V\left(\bigcap_j I_j\right)$$

Theorem 9.5. *If* $f\colon R \to S$ *is a ring homomorphism, then there is a continuous map*

$$f^{\#}\colon \operatorname{Spec} S \to \operatorname{Spec} R, \qquad f^{\#}(p) = f^{-1}(p)$$

Proof. Consider the exact sequence

$$0 \to f^{-1}(p) \to R \to S \to S/p \to 0.$$

Therefore $R/f^{-1}(p) \simeq S/p$ is a domain. Hence $f^{-1}(p)$ is prime.

To show $f^{\#}$ is continuous, consider ${f^{\#}}^{-1}(V(I))$ where I is an ideal in R. Let $q \in \operatorname{Spec} S$. Then

$$\begin{aligned} & q \in {f^{\#}}^{-1}(V(I)) \\ \Leftrightarrow\ & f^{\#}(q) \in V(I) \\ \Leftrightarrow\ & f^{-1}(q) \supset I \\ \Leftrightarrow\ & f(I) \subset q \\ \Leftrightarrow\ & Sf(I) \subset q \\ \Leftrightarrow\ & q \in V(Sf(I)). \end{aligned}$$

Thus ${f^{\#}}^{-1}(V(I)) = V(Sf(I))$. □

If $X \subset \mathbb{A}^n$, then

$$\mathcal{O}(X) = \frac{k[x_1, \cdots, x_n]}{I(X)}.$$

Definition 9.6. The category of **affine algebraic varieties over a field** k is the opposite of the category of finitely generated prime k-algebras with k-algebra homomorphisms.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 10: April 21

Maps Between Varieties

We're trying to find the "correct" maps between affine algebraic varieties. In the case $\mathbb{A}^n \to \mathbb{A}^1$, it would be natural to allow all polynomial functions on $k[x_1, \cdots, x_n]$. Notice that these can be redundant; for instance, take k to be finite. Then $k[x_1, \cdots, x_n]$ is infinite, but there are only finitely many functions. We can avoid this by assuming $k = \bar{k}$.

Definition 10.1. An **affine scheme** is a pair $(X, \mathcal{O}(X))$ where X is an affine algebraic variety.

In particular, $X = V(J) \subset \mathbb{A}^n_k$ and $\mathcal{O}(X) = k[x_1, \cdots, x_n]/J$.

Example 10.2. Let $X = \{pt\}$; the example is $(\operatorname{Spec} k, k)$. It consists of constant functions. Also $(\operatorname{Spec} \mathbb{R}, \mathbb{R}) \neq (\operatorname{Spec} \mathbb{C}, \mathbb{C})$.

Definition 10.3. If k is a field, the **affine line** over k, $\mathbb{A}^1_k$, is the pair $(\operatorname{Spec}(k[x]), k[x])$.

We don't care that in $k[x_1, \cdots, x_n]$, it is possible for different polynomials to be the same function. If $k = \bar{k}$, we don't have this problem; from now on, assume $k = \bar{k}$. The morphisms $f: \mathbb{A}^m_{(x_i)} \to \mathbb{A}^n_{(y_j)}$ are the functions induced by the ring homomorphisms

$$\phi: k[y_1, \cdots, y_n] \to k[x_1, \cdots, x_m].$$

So if $p = (a_1, \cdots, a_m) \in \mathbb{A}^m$, then $f(p) = (\phi(y_1)(p), \cdots, \phi(y_n)(p))$. Therefore **morphisms are tuples of polynomials**.

Given a closed $X \subset \mathbb{A}^n$, the morphisms from X to $\mathbb{A}^1$ are the restrictions of polynomials to X. There is a ring homomorphism from $k[x_1, \cdots, x_n]$ to the set of functions from $X \to k$, determined by $f \mapsto f|_X$. The kernel of this homomorphism is $I(X)$. So its image is $\mathcal{O}(X) \simeq k[x_1, \cdots, x_n]/I(X)$. Thus $\mathcal{O}(X)$ is the ring of regular functions on X.

We can extend to consider the morphisms from closed X to $\mathbb{A}^m_{(y_j)}$. Then they are the functions $p \mapsto (f_1(p), \cdots, f_m(p))$, where each $f_j \in \mathcal{O}(X)$. Such a function yields a homomorphism $k[y_1, \cdots, y_m] \to \mathcal{O}(X)$ by sending $y_i \mapsto f_i$, so that $g \mapsto g \circ f$ for $g \in k[y_1, \cdots, y_m]$.

Now consider $Y \subset \mathbb{A}^m$ closed. The morphisms from $X \to Y$ are the morphisms $f: X \to \mathbb{A}^m$ such that $f(X) \subset Y$. This gives rise to a homomorphism $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$; indeed, the induced homomorphism from $k[y_1, \cdots, y_m] \to \mathcal{O}(X)$ vanishes on $I(Y)$, so it passes to the quotient.

In more detail, suppose that $g \in I(Y)$. Then $g|_Y = 0$. Hence $g(f(p)) = 0$ for all $p \in X$. But $g \circ f: X \to k$, and $g \circ f|_X = 0$. Thus g is sent to 0, so the induced homomorphism vanishes on $I(Y)$.

Definition 10.4. If $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are closed, then the **morphisms from** $X \to Y$ are the maps induced by the k-algebra homomorphism $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$.

From now on, we think of the ring $\mathcal{O}(X)$ as the primary object.

Let R be a finitely generated k-algebra without nilpotents. If $R = k[t_1, \cdots, t_d]$, then we have a homomorphism $\phi: k[x_1, \cdots, x_d] \to R$ given by $\phi(x_i) = t_i$. This is surjective, and $R \simeq k[x_1, \cdots, x_d]/\ker\phi$. Since $\sqrt{0} = 0$, it follows that $\ker\phi$ is radical, so we can define $X \subset \mathbb{A}^d$ by $X = V(\ker\phi)$. Then $\mathcal{O}(X) \simeq R$.

There are many choices of generating sets for R, so there are many $X \subset \mathbb{A}^n$ for lots of different n such that $R \simeq \mathcal{O}(X)$. We declare all such X to be isomorphism; this point of view says that two affine varieties are isomorphic if $\mathcal{O}(X) \simeq \mathcal{O}(Y)$.

Example 10.5.

1. Take $\mathbb{A}^1, k[t]$ and the parabola $y = x^2$ in $\mathbb{A}^2_{x,y}$. Then

$$\mathcal{O}(\{y = x^2\}) = k[x,y]/(y - x^2) \simeq k[x],$$

where the latter is the ring of regular functions on $\mathbb{A}^1$ (the affine line). So the parabola is isomorphic to the line. Explicit maps from $\mathbb{A}^1$ to the parabola include $t \mapsto (t, t^2)$, and its inverse function $(x,y) \mapsto x$ for x on the parabola.

2. Take $\mathbb{A}^1$ and $k[t]$ again, and the cuspidal cubic $C = \{y^2 = x^3\}$ in $\mathbb{A}^2$. Then

$$\mathcal{O}(C) = k[x,y]/(y^2 - x^3) \not\simeq k[t],$$

because $\mathcal{O}(C)$ is not a PID. Indeed, let $\mathfrak{m} = (x,y) \subset \mathcal{O}(C)$. Then $\mathfrak{m}^2 = (x^2, xy, y^2) = (x^2, xy)$. Hence $\dim \mathfrak{m}/\mathfrak{m}^2 = 2$ as a k-vector space. If it were a PID, then the dimension would have to be 1 **(needs to be clarified!)**. If we draw the curve, the cusp at (0,0) corresponds to the non-principal maximal ideal $\mathfrak{m}$. However, every other point corresponds to a principal maximal ideal.

There are mutually inverse functions:

$$\mathbb{A}^1 \to C: t \mapsto (t^2, t^3) \qquad C \to \mathbb{A}^1: (x,y) \mapsto \begin{cases} yx^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases}.$$

The former corresponds to the homomorphism $k[x,y]/(y^2 - x^3) \to k[t]$, whereas the latter does not correspond to any ring homomorphism $k[t] \to k[x,y]/(y^2 - x^3)$. Thus it is not a morphism of varieties, so we don't have an isomorphism.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 11: April 23

Thinking of Varieties Abstractly

Here is one example to show the benefit. Consider $\mathcal{O}(X)$ for $X = \mathbb{A}^1 \setminus \{0\}$ which is not closed. Every element in $k[x, x^{-1}]$ gives a well-defined function from $\mathbb{A}^1 \setminus \{0\} \to k$. But it doesn't make sense a function on $\mathbb{A}^1$ due to the pole at the origin. Now

$$k[x, x^{-1}] \simeq k[x, y]/(xy - 1) = \mathcal{O}(\text{hyperbola}),$$

which is a closed subariety of $\mathbb{A}^2$.

There is a bijective map

$$\begin{aligned} X &\to \mathbb{A}^1 \setminus \{0\} \\ (x, y) &\mapsto x \\ (t, t^{-1}) &\leftarrow\!\shortmid t \end{aligned}$$

So although $\mathbb{A}^1 \setminus \{0\}$ is not a closed subvariety of $\mathbb{A}^1$, we will call it an affine variety because of this bijection. We enlarge our class of affine varieties in this manner.

Algebraic Groups

For example, $GL(n, k) \subset M_n(k) \simeq \mathbb{A}^{n^2}$. This is the open subspace (in the Zariski topology)

$$GL(n, k) = \mathbb{A}^{n^2} \setminus \{\operatorname{Ker} \det\}.$$

Thus $\mathcal{O}(\mathbb{A}^{n^2}) = \mathcal{O}(M_n(k)) = k[x_{ij} \mid 1 \le i, j \le n]$. Here $x_{ij}(a) = a_{ij}$. Thus $\mathcal{O}(M_n(k))[\det^{-1}]$ are all well-defined functions from $GL(n, k) \to k$. In addition,

$$\mathcal{O}(M_n(k))[\overset{-1}{\det}] \simeq \mathcal{O}(Y), \qquad Y = \{(a, \det a) \mid a \in M_n(k)\} \subset M_n(k) \times k.$$

Thus we think of $GL(n, k)$ as an affine algebraic variety (given by Y) above, which is a closed subspace of $M_n(k) \times k$.

Definition 11.1. If $X \subset \mathbb{A}^n$ is a closed subset, we will call $\mathcal{O}(X) = k[x_1, \cdots, x_n]/I(X)$ the **coordinate ring** of X.

Recap from last time:

Definition 11.2. If $X \subset \mathbb{A}^m, Y \subset \mathbb{A}^n$ are closed subvarieties, then a **morphism** from X to Y is a function $f: X \to Y$ of the form $f(p) = (f_1(p), \cdots, f_n(p))$ where $f_1, \cdots, f_n \in k[x_1, \cdots, x_m]$.

A function $f: X \to Y$ is a morphism if $y_i \circ f = f_i$ are polynomial functions on X, for all i.

From now on, **assume that** $k = \bar{k}$.

Definition 11.3. A k-algebra is called **reduced** if $\sqrt{0} = 0$.

Theorem 11.4. *The category of affine algebraic varieties and morphisms is anti-equivalent to the category of finitely generated reduced k-algebras and k-algebra homomorphisms.*

http://en.wikipedia.org/wiki/Algebraic_geometry#Morphism_of_affine_varieties.

Concretely, this says the following. Let $X \subset \mathbb{A}^m$, $Y \subset \mathbb{A}^n$ be closed subvarieties.

1. If $f: X \to Y$ is a morphism, then the function $f^*: \mathcal{O}(Y) \to \mathcal{O}(X)$ defined by $f^*(g) = g \circ f$ is a k-algebra homomorphism
2. if $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$ is a k-algebra homomorphism, then there is a unique morphism $f: X \to Y$ such that $\phi = f^*$.
3. If $f: X \to Y$ and $g: Y \to Z$ are morphisms, then $(g \circ f)^* = f^* \circ g^*$.
4. If $id_X: X \to X$ is the identity morphism, then $id_{\mathcal{O}(X)} = (id_X)^*$.

A rich dictionary between algebra and geometry

Definition 11.5. If $x \in X$, write

$$\begin{aligned} m_x &= I(\{x\}) \\ &= \text{ideal vanishing at } x \\ &= \operatorname{Ker} ev_x \end{aligned}$$

where $ev_x: \mathcal{O}(X) \to k$ is given by $ev_x(f) = f(x)$.

Note that m_x is a maximal ideal and $\mathcal{O}(X)/m_x \simeq k$.

Theorem 11.6. *Suppose $X \subset \mathbb{A}^m$, $Y \subset \mathbb{A}^n$ are closed. Let $f: X \to Y$ be a morphism and let $\phi = f^*: \mathcal{O}(Y) \to \mathcal{O}(X)$ be the corresponding algebra morphism.*

1. If $x \in X$, then $m_{f(x)} = \phi^{-1}(m_x)$
2. If $y \in Y$, then $f^{-1}(y) = V(\phi(m_y))$; $f^{-1}(y)$ is an affine variety.
3. $\operatorname{Ker}(\phi) = I(f(X))$ and $V(\operatorname{Ker}(\phi)) = \overline{f(X)}$
4. $\operatorname{Ker} \phi = 0$ if and only if $f(X) \subset Y$ is dense
5. If $Z \subset Y$ is closed, then $f^{-1}(Z) = V(\phi(I(Z))$ so is closed.
6. f is continuous

7. If $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module, then
   (a) the fibers of f are finite
   (b) if ϕ is injective, then f is surjective
   (c) if $Z \subset X$ is closed, then $f(Z) \subset Y$ is closed

Proof. 1. Let $g \in \mathcal{O}(Y)$. Then

$$\begin{aligned} & g \in \mathfrak{m}_{f(x)} \\ \Leftrightarrow\ & (g \circ f)(x) = 0 \\ \Leftrightarrow\ & f^*(g)(x) = 0 \\ \Leftrightarrow\ & \phi(g)(x) = 0 \\ \Leftrightarrow\ & \phi(g) \in \mathfrak{m}_x \end{aligned}$$

hence $\mathfrak{m}_{f(x)} = \phi^{-1}(\mathfrak{m}_x)$.
Alternate proof: $\mathcal{O}(Y) \to \mathcal{O}(X) \to k$, given by $h \mapsto h \circ f \mapsto h(f(x))$.

2. Let $x \in X$. If $x \in f^{-1}(y)$, then

$$\begin{aligned} & x \in f^{-1}(y) \\ \Leftrightarrow\ & f(x) = y \\ \Leftrightarrow\ & \mathfrak{m}_y = \phi^{-1}(\mathfrak{m}_x) \\ \Leftrightarrow\ & \phi(\mathfrak{m}_y) \subset \mathfrak{m}_x \\ \Longrightarrow\ & V(\phi(\mathfrak{m}_y)) \supset V(\mathfrak{m}_x) = \{x\} \\ \Leftrightarrow\ & x \in V(\phi(\mathfrak{m}_y)) \\ \Longrightarrow\ & f^{-1}(y) \subset V(\phi(\mathfrak{m}_y)). \end{aligned}$$

If $x \in V(\phi(\mathfrak{m}_y))$, then $\phi(\mathfrak{m}_y) \subset \mathfrak{m}_x$ so $\mathfrak{m}_y \subset \phi^{-1}(\mathfrak{m}_x)$ then $\mathfrak{m}_y = \phi^{-1}(\mathfrak{m}_x)$ and $y = f(x)$; thus $V(\phi(\mathfrak{m})) \subset f^{-1}(y)$.

□

Math 506 Modern Algebra Notes by Avi Levy

Lecture 12: April 25

Theorem 12.1. *If* $k = \bar{k}$, $f: X \to Y$, $\phi = f^*: \mathcal{O}(Y) \to \mathcal{O}(X)$, *then:*

(1) $x \in X \implies \mathfrak{m}_{f(x)} = \phi^{-1}(\mathfrak{m}_x)$

(2) $y \in Y \implies f^{-1}(y) = V(\phi(\mathfrak{m}_y))$

(3) $\operatorname{Ker}\phi = I(f(X))$ and $\overline{f(X)} = V(\operatorname{Ker}\phi)$

(4) $\operatorname{Ker}\phi = 0 \Leftrightarrow f(X)$ is dense in Y

(5) $Z \subset Y$ closed $\implies f^{-1}(Z) = V(\phi(I(Z))$ is closed

(6) f is continuous

(7) If $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module, then

   (a) the fibers of f are finite

   (b) ϕ injective $\implies$ f surjective

   (c) $Z \subset X$ is closed $\implies$ $f(Z)$ is closed

Proof. (3) If $g \in \mathcal{O}(Y)$, then

$$\begin{aligned} & \phi(g) = 0 \\ \Leftrightarrow\ & (g \circ f)(X) = 0 \\ \Leftrightarrow\ & g \in I(f(X)) \end{aligned}$$

(4) Since $\overline{f(X)} = V(I(f(X)) = V(\operatorname{Ker}\phi)$, it follows that $\operatorname{Ker}\phi = 0 \Leftrightarrow \overline{f(X)} = V(0) = Y$.

(5) For $x \in X$,

$$\begin{aligned} & x \in f^{-1}(Z) \\ \Leftrightarrow\ & f(x) \in Z = V(I(Z)) \\ \Leftrightarrow\ & g(f(x)) = 0, \qquad \forall g \in I(Z) \\ \Leftrightarrow\ & \phi(g)(x) = 0 \\ \Leftrightarrow\ & h(x) = 0 \qquad \forall h \in \phi(I(Z)) \\ \Leftrightarrow\ & x \in V(\phi(I(Z))). \end{aligned}$$

Thus $f^{-1}(Z) = V(\phi(I(Z)))$.

(6) Follows from (5) since f^{-1}(closed) is closed.

□

Before we prove (7), we remark on a special case. Consider $f: X \to X/G$ where G is a finite group acting as automorphisms of X. We had proven from Hilbert that $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(X)^G$-module.

Definition 12.2. X/G is defined to be the affine algebraic variety

$$\mathcal{O}(X/G) = \mathcal{O}(X)^G.$$

Note that $\mathcal{O}(X)$ is a finitely generated k-algebra, so it is the coordinate ring of some affine algebraic variety, which we call "X/G". To justify the notation, there are some things to show; for instance, the inclusion $\mathcal{O}(\text{“}X/G\text{”}) \simeq \mathcal{O}(X)^G \hookrightarrow \mathcal{O}(X)$ gives a morphism from $f: X \to$ "X/G". We need to show that f is surjective, with fibers the G-orbits. Then we are justified claiming that we are the coordinate ring of X/G.

Suppose G acts on a topological space X, and $\pi: X \to X/G$ is the canonical projection. Then the quotient topology on X/G is characterized by the property:

Proposition 12.3 (Universal property for coset space)**.** *For any continuous map $h: X \to Y$ with fibers the orbits of G, there is a unique continuous $\tilde{h}: X/G \to Y$ such that $h = \tilde{h} \circ \pi$.*

Let $\phi = f^*$, where f is the morphism $f: X \to$ "X/G" and

$$\phi: \mathcal{O}(\text{“}X/G\text{”}) \simeq \mathcal{O}(X)^G \hookrightarrow \mathcal{O}(X).$$

If $h: X \to Y$ is a morphism that is constant on the fibers, then there is a unique morphism $\tilde{h}:$ "X/G" $\to X$ such that $h = \tilde{h} \circ f$. Some more work we'll do next time...

Then it follows that $\mathcal{O}(X/G) \simeq \mathcal{O}(X)^G \subset \mathcal{O}(X)$; consequently $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(X/G)$-module with finite fibers, so (7) applies.

Example 12.4. Consider the cuspidal cubic $k[t^2, t^3] \subset k[t]$; visualize this as a map

$$f: \mathbb{A}^1 \to \{\text{cuspidal cubic}\}.$$

Then f is bijective, so we can consider

$$\mathbb{A}^1 \sqcup \mathbb{A}^1 \to \mathbb{A}^1 \to \{\text{cuspidal cubic}\},$$

and a map σ that interchanges the two copies of $\mathbb{A}^1$ in the first space.

Before we return to a proof of (7), we need a lemma:

Lemma 12.5. *Let R be finite dimensional k-algebra. Then R has only finitely many maximal ideals.*

Proof. Take a composition series

$$R \supset I_1 \supset \cdots \supset I_n = 0.$$

Each I_j/I_{j+1} is a simple R-module, and every simple R-module appears in this list. Hence R has only finitely many simple modules, and therefore only finitely many maximal ideals. If $m \neq n$ are maximal, then $R/m \not\simeq R/n$ (by checking annihilators). □

Corollary 12.6. *If $\mathcal{O}(W)$ is finite dimensional, then $|W| < \infty$.*

At long last, a proof of (7):

Proposition 12.7 (Item (7) of big theorem)**.** *If $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module, then*

(a) the fibers of f are finite

(b) ϕ injective $\implies$ f surjective

(c) $Z \subset X$ is closed $\implies$ $f(Z)$ is closed

Proof. To ease notation, set $R = \mathcal{O}(X)$ and $S = \mathcal{O}(Y)$.

(a) For $y \in Y$,

$$f^{-1}(y) = V(\phi(\mathfrak{m}_y)) = V(R\phi(\mathfrak{m}_j)).$$

R is a finitely generated S-module, so $R/R\phi(\mathfrak{m}_y)$ is a finitely generated S-module and thus a finitely generated $S/\mathfrak{m}_g$-module. Hence $\dim_k(R/R\phi(\mathfrak{m}_y)) < \infty$.

Finite dimensional k-algebras have only a finite number of maximal ideals, so $V(R\phi(\mathfrak{m}_y))$ is finite.

□

Math 506 Modern Algebra Notes by Avi Levy

Lecture 13: April 28

Dominant Morphisms

Definition 13.1. A morphism $f: X \to Y$ is **dominant** if $\overline{f(X)} = Y$. By the theorem, $f: X \to Y$ is dominant if and only if the corresponding algebra homomorphism $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective.

Example 13.2. Some pictures:

$k[x, x^{-1}] \simeq k[x, y]/(xy - 1)$.

$\varphi: k[x] \to k[x, y]/(xy - 1)$

$f: \{xy = 1\} \to \mathbb{A}^1$, $(x, y) \to x$

Now the proof: If $\psi_1, \psi_2: k[x, x^{-1}] \to R = \mathcal{O}(Y)$ are ring homomorphisms such that $\psi_1\varphi = \psi_2\varphi$, then $\psi_1(x) = \psi_2(x)$ and $\psi_i(x^{-1}) = \psi_i(x)^{-1}$. Then $\psi_1(x^{-1}) = \psi_2(x^{-1})$, so $\psi_1 = \psi_2$.

The idea behind the example is that f has the cancellation property: if $g_1, g_2: Y \to C$, $Y \to_{g_i} C \to_f \mathbb{A}^1$ (i.e. $fg_1 = fg_2$), then $g_1 = g_2$. This is what it means for f to be dominant; it need not be surjective, so you can not cancel it on the grounds of set theory.

In the category of topological spaces if $g_1, g_2: Y \to C$ are continuous and agree on a dense subset $U \subset Y$, then $g_1 = g_2$.

In the earlier example: f is injective and a monomorphism. Also f is surjective, but it is not an epimorphism. Similarly $\varphi: k[x] \to k[x, x^{-1}]$ is not surjective but it is an epimorphism.

Function fields

We introduce the function field of an irreducible affine variety in the case $k = \bar{k}$. Let $X \subset \mathbb{A}^n$ be irreducible. Then $\mathcal{O}(X)$ is a domain so it has a field of fractions,

$$k(X) = \left\{ \frac{g}{h} \mid g, h \in \mathcal{O}(X), h \neq 0 \right\}.$$

Definition 13.3. $k(X)$ is called the **ring of rational functions on** X.

If $f: X \to Y$ is a dominant morphism between irreducible varieties, there is a commuting diagram of injective algebra homomorphisms

$$\begin{array}{ccc} \mathcal{O}(Y) & \xhookrightarrow{\varphi} & \mathcal{O}(X) \\ \downarrow & & \downarrow \\ k(Y) & \hookrightarrow & k(X). \end{array}$$

The downward arrows are $R \to R[S^{-1}]$ where S is the multiplicative set.

Open subsets of affine varieties

If $0 \neq f \in \mathcal{O}(X)$ and f is not a unit, we write $X_f = X \setminus V(f)$, which is open.

Definition 13.4. X_f is called a **principal** or **basic** open set.

Consider $X_f \subset \mathbb{A}^n$, so that $I = I(X_f) \subset k[x_1, \cdots, x_n]$. Make X_f into the affine variety $V(I, fx_{n+1} - 1) \subset \mathbb{A}^{n+1}$ (we justify this in the following proposition).

Proposition 13.5. *The inclusion $X_f \hookrightarrow X$ is a morphism of affine varieties.*

Proof. It makes sense to give X_f the structure of $V(I, fx_{n+1} - 1)$, because we have the set isomorphism

$$X_f \longleftrightarrow V(I, fx_{n+1} - 1)$$

$$p \longmapsto (p, f(p)^{-1}).$$

Then the diagram $V(I, fx_{n+1} - 1) \to \mathbb{A}^{n+1}$ commutes with $X \hookrightarrow \mathbb{A}^n$ when projected down. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 14: April 30

Proposition 14.1. *Let R be a subring of S, where S is a finitely generated R-module. If $\mathfrak{m}$ is a maximal ideal of R, there is a maximal ideal $\mathfrak{n} \subset S$ such that $R \cap \mathfrak{n} = \mathfrak{m}$.*

Proof. Write $S = \sum_{j=1}^{n} Rs_j$, and assume $s_1 = 1$. It suffices to show that $S\mathfrak{m} \neq S$, because then $S\mathfrak{m}$ is contained in some maximal ideal $\mathfrak{n} \subset S$, and then $1 \notin \mathfrak{n} \cap R \supset \mathfrak{m}$ so $\mathfrak{n} \cap R = \mathfrak{m}$. Suppose to the contrary that $S\mathfrak{m} = S$. Then $S\mathfrak{m} = \sum_{i=1}^{n} Rs_i$, so each $s_i = \sum_{j=1}^{n} s_j x_{ij}$ for some $x_{ij} \in \mathfrak{m}$. Hence

$$\sum_{j=1}^{n} (\delta_{ij} - x_{ij}) s_j = 0.$$

Let $M = (\delta_{ij} - x_{ij})$; then $\det M = 0$. But expanding the determinant yields

$$0 = \det \begin{pmatrix} 1 - x_{11} & \cdots & -x_{1n} \\ \vdots & \ddots & \vdots \\ -x_{n1} & \cdots & 1 - x_{nn} \end{pmatrix} = 1 + d,$$

where d involves only x_{ij} expressions, so $d \in \mathfrak{m}$. Thus $1 \in \mathfrak{m}$, which is a contradiction. □

Finite morphisms

Let X, Y be irreducible affine varieties.

Definition 14.2. We say that a morphism $f: X \to Y$ is **finite** when $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module.

If $f: X \to Y$ is surjective, then using the diagram

$$\begin{array}{ccc} \mathcal{O}(X) & \longleftarrow & \mathcal{O}(Y) \\ \downarrow & & \downarrow \\ k(X) & \longleftarrow & k(Y) \end{array}$$

shows that $k(X)$ is a $k(Y)$-vector space.

Definition 14.3. The **degree** of a finite surjective morphism $f: X \to Y$ is $\dim_{k(Y)} k(X)$.

Theorem 14.4. *Let $f: X \to Y$ be a finite dominant morphism. If $\mathcal{O}(X)$ is generated by t elements as an $\mathcal{O}(Y)$-module, then*

(1) $|f^{-1}(y)| \leq t, \qquad \forall y \in Y$

(2) f *is surjective*

(3) f *sends closed sets to closed sets*

Proof. (2) Since f is dominant, the corresponding homomorphism $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective. Hence we may view $\mathcal{O}(Y)$ as a subalgebra of $\mathcal{O}(X)$.

Let $\mathfrak{m}$ be the maximal ideal in $\mathcal{O}(Y)$ that vanishes at y. By the proposition, there is a maximal ideal $\mathfrak{n} \subset \mathcal{O}(X)$ such that $\mathfrak{n} \cap \mathcal{O}(Y) = \mathfrak{m}$. Then $f^{-1}(y) = V(\mathfrak{m}\mathcal{O}(X)) \supset V(\mathfrak{n}) \neq \varnothing$, so f is surjective.

(1) We have the diagram

$$\begin{array}{ccccccc} & & \mathcal{O}(Y) & \longrightarrow & \mathcal{O}(X) & & \\ & & \downarrow & & \downarrow & & \\ \mathcal{O}(\{y\}) & = & \mathcal{O}(Y)/\mathfrak{m} & \longrightarrow & \mathcal{O}(X)/\mathfrak{m}\mathcal{O}(X) & = & \mathcal{O}(f^{-1}(y)) \end{array}$$

Thus $\mathcal{O}(f^{-1}(y))$ is a finitely generated $\mathcal{O}(Y)/\mathfrak{m}$-module, i.e. a finite dimensional vector space. Now since $\dim \mathcal{O}(X)/\mathfrak{m}\mathcal{O}(X) \leq t$, our composition series has length at most t. Now every simple module must appear, so there are at most t simples; but these are in bijection with the maximal ideals. Thus $|f^{-1}(y)| \leq t$.

(3) Let $Z \subset X$ be closed. To show that $f(Z)$ is closed, it suffices to show that $f|_X: Z \to \overline{f(Z)}$ is surjective. This follows from (2), since the homomorphism ϕ corresponding to $f|_Z$ fits into the commutative diagram

$$\begin{array}{ccccccc} & & \mathcal{O}(Y) & \xrightarrow{\phi} & \mathcal{O}(X) & & \\ & & \downarrow & & \downarrow & & \\ \mathcal{O}(\overline{f(Z)}) & = & \mathcal{O}(Y) & \longrightarrow & \mathcal{O}(Z) & = & \mathcal{O}(X)/I(Z) \end{array}$$

Since $\mathcal{O}(X)$ is generated by $\leq t$ elements as an $\mathcal{O}(Y)$-module, $\mathcal{O}(Z)$ is generated by $\leq t$ elements as an $\mathcal{O}(\overline{f(Z)})$-module. Using (2), $f(Z) = \overline{f(Z)}$.

To elaborate on the proof of (3), recall that earlier we had $f: X \to Y$ and $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$. Then we showed $I(\overline{f(Z)}) = \phi^{-1}(I(Z))$; then $I(\overline{f(X)}) = \ker \phi$. □

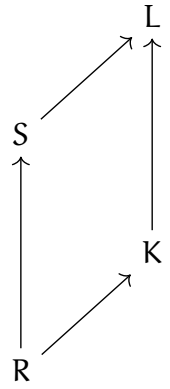
Math 506 Modern Algebra Notes by Avi Levy

Lecture 15: May 2

$$\begin{array}{ccc} X & \mathcal{O}(X) & k(X) \\ \downarrow f & \uparrow & \uparrow \\ Y & \mathcal{O}(Y) & k(Y) \end{array}$$

We proved that if $\mathcal{O}(X)$ is finitely generated by $\leq t$ elements as an $\mathcal{O}(Y)$-module, then $|f^{-1}(y)| \leq t$.

Lemma 15.1. *Let S be a domain, $R \subset S$. Set $K = \operatorname{Frac} R = \operatorname{Frac} S$. If S is generated by t elements as an R-module, then $\dim_K L \leq t$ and there are elements in S that form a basis for L as a K-vector space.*



Proof. $S = Rs_1 + \cdots + Rs_t$. Then $Ks_1 + \cdots + Ks_t \subset L$. Hence

$$s_i s_j = \sum_{p=1}^{t} r_{pij} s_p \in Ks_1 + \cdots + Ks_t,$$

for some $r_{pij} \in R$. Hence $Ks_1 + \cdots + Ks_t$ is a ring, a domain (as a subring of L), and a finite dimensional vector space over K. Thus it is a field. Since it contains S, $Ks_1 + \cdots + Ks_t = L$; therefore some subset of $\{s_1, \cdots, s_t\}$ is a K-basis for L. □

Definition 15.2. The **degree** of a finite dominant morphism $f: X \to Y$ is $\dim_{k(Y)} k(X)$.

Theorem 15.3. *If $f: X \to Y$ is a finite dominant morphism between irreducible varieties, then $|f^{-1}(y)| \leq \deg f$ and equality occurs for some y.*

A simple example in the plane is $y^2 = x(x-1)(x-\lambda)$. Then the real slice of the curve looks like a loop and a line. Consider the morphism π that projects to the x-axis. Algebraically, we are looking at

$$\begin{array}{ccc} k[x] & \hookrightarrow & k[x,y]/(y^2 - x(x-1)(x-\lambda)) \\ \vdots & & \vdots \\ \text{Frac} & & \text{Frac} \\ \downarrow & & \downarrow \\ k(x) & \hookrightarrow & k(x) \oplus k(x)y \end{array}$$

On most points the degree is 2, but sometimes it isn't; this is because we're losing out by looking at $\mathbb{R}$ and not in $\mathbb{C}$.

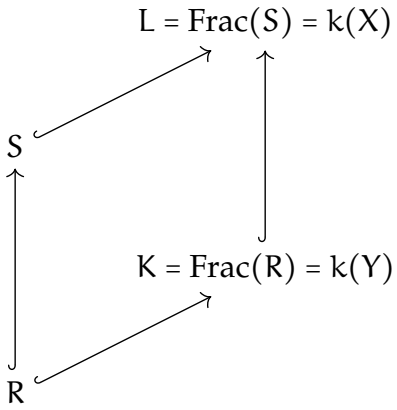
Math 506 Modern Algebra Notes by Avi Levy

Lecture 16: May 5

Theorem 16.1. *Let $f: X \to Y$ be a finite dominant morphism between irreducible varieties. Then*

$$|f^{-1}(y)| \leq \deg f, \qquad \forall y \in Y.$$

Proof. Let $R = \mathcal{O}(Y), S = \mathcal{O}(X)$. Then $R \hookrightarrow S$ so we identify R with a subalgebra of S.



Last time, we showed that L has a basis over K consisting of elements $f_1, \cdots, f_n \in S$. Replace f_1 with 1,without loss of generality. Then

$$R \subset Rf_1 + \cdots + Rf_n \subset S, \qquad M = \frac{S}{Rf_1 + \cdots + Rf_n}.$$

Let $s \in S$ and write $\overline{s}$ for its image in M. Now $s = a_1 f_1 + \cdots + a_n f_n$ for some $a_i \in K$. Put everything over a common denominator $0 \neq x \in R$; then $xs \in Rf_1 + \cdots + Rf_n$, so $x\overline{s} = 0$. Hence $\mathrm{Ann}(\overline{s_i}) \neq 0$.

Since f is a finite morphism, S and therefore M is an fg R-module. If $\overline{s_1}, \cdots, \overline{s_t}$ generate M as an R-mod,

$$\begin{aligned} \mathrm{Ann}_R(M) &= \bigcap_{i=1}^{t} \mathrm{Ann}_R(\overline{s_i}) \\ &\supset \prod_{i=1}^{t} \mathrm{Ann}(\overline{s_i}) \\ &\neq 0. \end{aligned}$$

This uses the fact that R is a domain, since our variety Y is irreducible.

Now write $J = \mathrm{Ann}_R(M)$. Since $J \neq 0$, $Y \setminus V(J)$ is a dense subset of Y. Let $y \in Y \setminus V(J)$, and m_y is the maximal ideal in R vanishing at y. Since $y \notin V(J)$, $J + m_y = R$. But then

$$\mathrm{Ann}\left(\frac{S}{Rf_1 + \cdots + Rf_n + Sm_y}\right) = J + m_y = R.$$

Hence $S = Rf_1 + \cdots + Rf_n + Sm_y$; thus as an R-module, S/Sm_y is generated by n elements. Then S/Sm_y is an R/m_y-module, also generated by n elements; hence

$$\dim_{R/m_y}(S/Sm_y) \leq n.$$

Thus S/Sm_y has at most n maximal ideals, which means $|f^{-1}(y)| \leq n$.

To extend from a dense set to all of Y, we need to repeat the argument using this sort of diagram:

$$\begin{array}{ccc} \cdots & f^{-1}(V(J)) & \hookrightarrow X \\ & \downarrow f & \downarrow f \\ \cdots & V(J) & \hookrightarrow Y \end{array}$$

Then we use the noetherian condition to show that after finitely many steps, there are no more strictly decreasing dense subsets. We skipped the gory details. □

If $X, Y \subset \mathbb{A}^m, \mathbb{A}^n$ are closed, then $X \times Y \subset \mathbb{A}^{m+n}$ is closed. Let $I(X) \subset k[x_1, \cdots, x_m]$ be the ideal vanishing on X, and same for $I(Y) \subset k[y_1, \cdots, y_n]$. Then $k[x_1, \cdots, x_m, y_1, \cdots, y_n] = A$ is a coordinate ring for $\mathbb{A}^{m+n}$. Then $I(X \times Y)$, the functions in A that vanish on $X \times Y$, is $AI(X) + AI(Y)$.

Let $\sum f_i g_i \in A$ where $f_i \in k[x_1, \cdots, x_m]$ and $g_i \in k[y_1, \cdots, y_n]$. If $(x, y) \in X \times Y$, then

$$\left(\sum f_i g_i\right)(x, y) = \sum f_i(x) g_i(y).$$

If all $f_i \in I(X)$ or all $g_i \in I(Y)$, then the sum vanishes. Hence $AI(X) + AI(Y) \subset I(X \times Y)$.

If for each i, at least one of $f_i \in I(X)$ or $g_i \in I(Y)$, then $\sum f_i g_i \in AI(X) + AI(Y)$. Hence if $\sum f_i g_i \notin AI(X) + AI(Y)$, there is some i such that $f_i \notin I(X)$ and $g_i \notin I(Y)$.

Consider $p \in \mathbb{A}^m \mid f_i(p) \neq 0\}$ is open for all i. Since $f_i \neq 0$ it is non-empty, and hence dense in $\mathbb{A}^m$.

Proposition 16.2. $I(X \times Y) = AI(X) + AI(Y)$

Corollary 16.3. $X \times Y$ *is closed in* $\mathbb{A}^{m+n}$

Tensor products

$k[x_1, \cdots, x_m, y_1, \cdots, y_n] = k[x_1, \cdots, x_m] \otimes_k k[y_1, \cdots, y_n]$.

Lemma 16.4. *If V, W are vector spaces over k with bases $\{v_i\}, \{w_j\}$ then $v_i \otimes w_j$ is a basis for $V \otimes_k W$.*

As a consequence, $\mathcal{O}(X \times Y) \simeq \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$; the set-theoretic operation $\times$ corresponds to the algebraic operation $\otimes$.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 17: May 7

Proposition 17.1. *Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be closed subvarieties. Then $X \times Y$ is a closed subvariety of $\mathbb{A}^{m+n}$ and $\mathcal{O}(X \times Y) \simeq \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$. Moreover, if X, Y are irreducible then so is $X \times Y$.*

Proof. Let $I(X) = (f_1, \cdots, f_p) \subset k[x_1, \cdots, x_m] = \mathcal{O}(\mathbb{A}^m)$ and $I(Y) = (g_1, \cdots, g_q) \subset k[y_1, \cdots, y_n] = \mathcal{O}(\mathbb{A}^n)$. Let $(x, y) \in \mathbb{A}^m \times \mathbb{A}^n$. Then

$$\begin{aligned}
&(x, y) \in X \times Y \\
&\Leftrightarrow x \in X, y \in Y \\
&\Leftrightarrow f_1(x) = \cdots = f_p(x) = 0, \qquad g_1(y) = \cdots = g_q(y) = 0 \\
&\Leftrightarrow f_1(x, y) = \cdots = f_p(x, y) = 0, \qquad g_1(x, y) = \cdots = g_q(x, y) = 0,
\end{aligned}$$

where we think of $f_i, g_j \in k[x_1, \cdots, x_m, y_1, \cdots, y_n] \simeq \mathcal{O}(\mathbb{A}^m) \otimes \mathcal{O}(\mathbb{A}^n)$. Thus $V(I) = X \times Y$, where $I = (f_1, \cdots, f_p, g_1, \cdots, g_p)$. Hence $X \times Y$ is closed in $\mathbb{A}^{m+n}$.

Claim 17.2. $I = I(X \times Y)$

Proof. We have shown that $I \subset I(X \times Y)$. For the reverse inclusion, suppose to the contrary that there is an $h \in I(X \times Y) \smallsetminus I$. Write $h = \sum_{i \le r} a_i \otimes b_i$ where $a_i \in \mathcal{O}(\mathbb{A}^m)$ and $b_i \in \mathcal{O}(\mathbb{A}^n)$ with r minimal. Then $\{b_1, \cdots, b_r\}$ are linearly independent, and

$$\{a_i\}_{i \le r} \notin I(X), \qquad \{b_i\}_{i \le r} \notin I(Y).$$

Now there is an $x \in X$ such that $a_i(X) \neq 0$. If $y \in Y$, then

$$0 = h(x, y) = a_1(x)b_1(y) + \cdots + a_r(x)b_r(y).$$

Hence $a_1(x)b_1 + \cdots + a_r(x)b_r \in I(Y)$. Then

$$b_1 = \frac{-1}{a_1(x)} \left(a_2(x)b_2 + \cdots + a_r(x)b_r\right) + g,$$

for $g \in I(Y)$. So we may write

$$h = a_1 \otimes \left(g - \frac{1}{a_1(x)} \left(a_2(x)b_2 + \cdots + a_r(x)b_r\right)\right) + \cdots + a_r \otimes b_r.$$

Since $g \in I(Y) \subset I \subset I(X \times Y)$, the element

$$\left(\frac{-a_2(x)}{-a_1(x)}a_1 + a_2\right) \otimes b_3 + \cdots + \left(\frac{-a_r(x)}{-a_1(x)}a_1 + a_r\right) \otimes b_r \in I(X \times Y) \smallsetminus I,$$

contradicting minimality of r. □

Consequently,

$$I(X \times Y) = I = I(X) \otimes \mathcal{O}(\mathbb{A}^n) + \mathcal{O}(\mathbb{A}^m) \otimes I(Y).$$

Therefore

$$\begin{aligned}\mathcal{O}(X \times Y) &= \frac{\mathcal{O}(\mathbb{A}^{m+n})}{I(X \times Y)} \\ &= \frac{\mathcal{O}(\mathbb{A}^m) \otimes_k \mathcal{O}(\mathbb{A}^n)}{I(X) \otimes_k \mathcal{O}(\mathbb{A}^n) + \mathcal{O}(\mathbb{A}^m) \otimes_k I(Y)}.\end{aligned}$$

□

To show that this completes the proof of the proposition, we need the following lemma.

Lemma 17.3. *If $U \subset V$ and $U' \subset V'$ are k-vector spaces, the map*

$$\Phi\colon \frac{V}{U} \otimes_k \frac{V'}{U'} \to \frac{V \otimes V'}{U \otimes V' + V \otimes U'}, \qquad \overline{x} \otimes \overline{y} = \overline{x \otimes y},$$

is an isomorphism of k-vector spaces.

Once we have this lemma, it follows that

$$\mathcal{O}(X \times Y) \simeq \frac{\mathcal{O}(\mathbb{A}^m)}{I(X)} \otimes \frac{\mathcal{O}(\mathbb{A}^n)}{I(Y)}.$$

Proof. There is a well-defined bilinear function on $\frac{V}{U} \times \frac{V'}{U'}$ defined by $\tilde{\Phi}(x, y) = \overline{x \otimes y}$. Since $\tilde{\Phi}(x\lambda, y) = \tilde{\Phi}(x, \lambda y)$ for all $\lambda \in k$, it follows that $\tilde{\Phi}$ induces a linear map on the tensor products. Keep running this argument over and over to show that various things are actually defined (i.e., vanish on the defining relations of the tensor product). Then define its inverse map $\Psi\colon V \otimes V' \to \frac{V}{U} \otimes \frac{V'}{U'}$ by $\Psi(x \otimes y) = \overline{x} \otimes \overline{y}$. Since $U \otimes V' + V \otimes U' \subset \ker \Psi$, it induces a linear map on the tensor product. □

Definition 17.4. If R, S are k-algebras, then so is $R \otimes_k S$ under the product $(a \otimes b)(c \otimes d) = ac \otimes bd$. Then we can think of $r_1 \otimes s_1 + \cdots + r_n \otimes s_n$ as $r_1 s_1 + \cdots + r_n s_n$.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 18: May 9

First a couple small general lemmas.

Lemma 18.1. *Let R be a ring and M a left R-module. Then the function*

$$\Phi: R \otimes_R M \to M, \qquad Rx \otimes m \mapsto xm$$

is an isomorphism of left R-modules.

Lemma 18.2. *Let V, V' be vector spaces and $U \subset V$ a subspace. Then*

$$\frac{V \otimes V'}{U \otimes V'} \simeq \frac{V}{U} \otimes V', \qquad \overline{v \otimes v'} \mapsto \overline{v} \otimes v'.$$

We've seen how to prove these sorts of little tensor product lemmas; you always make a function, then pass to the quotient in the definition of the tensor product.

Proposition 18.3. *Let R and S be finitely generated algebras. If R, S are domains, then so is $R \otimes_k S$.*

Proof. Let $x, y \in R \otimes S$ and suppose $xy = 0$. Write $x = \sum a_i \otimes b_i$, $y = \sum c_j \otimes d_j$. We can assume that the b_i's and d_j's are all linearly independent. Let m be a maximal ideal in R, and write $\overline{a_i}$ for the image of a_i in R/m_p. Thus

$$\begin{aligned} 0 &= \overline{xy} \\ &= \left(\sum \overline{a_i} \otimes b_i\right)\left(\sum \overline{c_j} \otimes d_j\right) \\ &\in R/m_p \otimes_k S \\ &\simeq k \otimes_k S \\ &\simeq S, \end{aligned}$$

where the $\simeq$ means "isomorphic as a k-algebra". It follows that

$$0 = \left(\sum \overline{a_i} b_i\right)\left(\sum \overline{c_j} d_j\right).$$

Since S is a domain, one of them is 0. Since the b_i's and d_j's are linearly independent, either all the a_i's are in m_p or all the c_j's are in m. Therefore

$$m_p \in V(a_1, \cdots) \cup V(c_1, \cdots).$$

There's some ambiguity in V; it means something in the original sense (vanishing locus), but it also means something in the "Spec" sense (sets of ideals). Here we are using the second sense.

Let Z denote the affine variety for which $R \simeq \mathcal{O}(Z)$. Repeating our argument for all $p \in Z$,

$$Z \subset V(a_1, \cdots) \cup V(c_1, \cdots).$$

But R is a domain, so Z is irreducible. Thus Z is one of $V(a_1, \cdots)$ or $V(c_i, \cdots)$; hence either $(a_1, \cdots) = 0$ or $(c_1, \cdots) = 0$, whereupon $x = 0$ or $y = 0$. □

Proposition 18.4. *Let* $f: X \to Y$ *be a morphism and define*

$$\Gamma_f = \{(x, f(x)) : x \in X\} \subset X \times Y$$

Then Γ_f *is an algebraic variety.*

Proof. f corresponds to a k-algebra homomorphism $\phi: \mathcal{O}(Y) \to \mathcal{O}(X)$. Let I be the ideal in $\mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ generated by

$$\{\phi(g) \otimes 1 - 1 \otimes g : g \in \mathcal{O}(Y)\}.$$

Then

$$\begin{aligned} V(I) &= \{(x, y) \in X \times Y : (\phi(g) \otimes 1 - 1 \otimes g)(x, y) = 0, \qquad \forall g \in \mathcal{O}(Y)\} \\ &= \{(x, y) : \phi(g)(x) - g(y) = 0, \qquad \forall g\} \\ &= \{(x, y) : g(f(x)) = g(y) \forall g\} \\ &= \{(x, y) : f(x) = y\}, \end{aligned}$$

by the nullstellensatz. The latter set is Γ_f, so we're done. □

We can continue along this theme of showing that various sets are "closed". For instance, show that two morphisms f, g agree on a closed set.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 19: May 14

Tangent Spaces

Fix a point p on an affine variety $X \subset \mathbb{A}^n$. We're going to look at lines through p.

Definition 19.1. If $q \in k^n \simeq \mathbb{A}^n$, the **line through** p in the **direction** q is

$$L_q = \{p + \lambda q : \lambda \in k\} = p + kq.$$

Suppose $I(X) = (f_1, \cdots, f_m) \subset k[x_1, \cdots, x_n]$. Introduce a new variable t, and consider the polynomials

$$f_j(p + tq) = f_j(p_1 + tq_1, \cdots, p_n + tq_n).$$

Why does he do this? Well a line in n-space is a map

$$\mathbb{A}^1 \longrightarrow \mathbb{A}^n$$

$$k[t] \longleftarrow k[x_1, \cdots, x_n]$$

$$p_j + tq_j \longleftarrow\!\shortmid\; x_j$$

$$f_i(p + tq) \longleftarrow\!\shortmid\; f_i$$

The map corresponds to $\mathbb{A}^1 \to L_q \subset \mathbb{A}^n$. Let $J = (\{f_i(p + tq)\}) \subset \mathbb{A}^1$, which is principal. Thus we may write it as $J = (f)$, where we explicitly have

$$f(t) = \gcd\{f_j(p + tq)\}.$$

Lemma 19.2. *With f as above,*

$$L_q \cap X = \{p + \lambda q : f(\lambda) = 0\}.$$

Proof. Let $x \in L_q \cap X$. Then $x = p + \lambda q$ for some $\lambda \in k$. Since $x \in X$, all f_i vanish at x; hence

$$f_i(p + \lambda q) = 0, \qquad \forall i.$$

Thus $t - \lambda$ divides $f_j(p + tq)$ for all j, so $f(\lambda) = 0$.

Conversely, suppose that $f(\lambda) = 0$, and let $x = p + \lambda q$. Since $t - \lambda \mid f(t)$, it follows that $t - \lambda$ divides each $f_j(p + tq)$. Hence each $f_j(p + \lambda q)$ vanishes, so $x \in X$. □

Definition 19.3. The **intersection multiplicity** of X and L_q at $p \in X$ is the multiplicity of the root 0 of $f(t)$. We say that L_q is **tangent** to X at p if the intersection multiplicity of X and L_q at p is ≥ 2. The **tangent space** to X at p is the subspace

$$T_pX = \{q \in k^n : L_q \text{ is tangent to } X \text{ at } p\} \cup \{0\} \subset k^n \simeq \mathbb{A}^n.$$

Some things to check. First, the polynomial $f(t)$ does not depend (up to scalar multiples) on the choice of generators for $I(X)$. Indeed, $(f) \subset k[t]$ is $\phi(I(X))$ (where ϕ is the homomorphism corresponding to $\mathbb{A}^1 \to \mathbb{A}^n$).

Our goal is to describe T_pX directly in terms of X (that is, in terms of the generators $f_1, \cdots, f_m$). Similarly, we would like to describe T_pX in terms of $\mathcal{O}(X)$ and p. To this end, we start talking about (formal) derivatives.

Notice that the partial derivatives $\frac{\partial}{\partial x_j} : \mathbb{A}^n \to \mathbb{A}^n$ make sense, in characteristic 0. Aside: In characteristic p, we have to use a "divided power" that is like a normalized derivative. Otherwise, factorials would crop up and cause issues like

$$\left(\frac{\partial}{\partial x}\right)^p = 0.$$

Definition 19.4. The **Taylor expansion** of a polynomial $g \in k[x_1, \cdots, x_n]$ around $p = (\alpha_1, \cdots, \alpha_n)$:

$$g = g(p) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}(p)(x - \alpha_i) + \frac{1}{2} \sum_{i,j=1}^{n} \frac{\partial^2 g}{\partial x_i \partial x_j}(p)(x - \alpha_i)(x - \alpha_j) + \cdots$$

Writing $I(X) = (f_1, \cdots, f_m)$, we take $p = (\alpha_1, \cdots, \alpha_n) \in X$ and $q = (\beta_i)$. Then

$$f_r(p + tq) = 0 + \sum_{i=1}^{n} \frac{\partial f_r}{\partial x_i}(p)(t\beta_i) + \frac{1}{2} \sum_{i,j=1}^{n} \frac{\partial^2 f_r}{\partial x_i \partial x_j}(p)(t\beta_i)(t\beta_j) + \cdots$$

Hence t^2 divides f_r precisely when

$$\sum_{i=1}^{n} \frac{\partial f_r}{\partial x_i}(p)\beta_i = 0.$$

Consequently $q \in T_pX$ precisely when that sum vanishes for all $i \leq r$. This is equivalent to saying

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(p) & \cdots & \frac{\partial f_1}{\partial x_n}(p) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(p) & \cdots & \frac{\partial f_m}{\partial x_n}(p) \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = 0.$$

Definition 19.5. This is the **Jacobian matrix** J_p of f at p.

Proposition 19.6. $q \in T_pX$ *if and only if* $J_p q = 0$*; thus* $T_pX = \ker(J_p)$.

In particular, T_pX is a subspace of $k^n \simeq \mathbb{A}^n$, of dimension $n - \operatorname{rank}(J_p)$. A priori, $\operatorname{rank}(J_p)$ can be different at different points p.

Examples

Are irreducible polynomials of constant rank? Consider $f = x^3 + y^3 + z^3 - \lambda xyz$. Set $X = V(f) \subset \mathbb{A}^3$. Then

$$J(f) = (3x^2 - \lambda yz, 3y^2 - \lambda xz, 3z^2 - \lambda xy).$$

Hence $J(f)(0,0,0) = (0,0,0)$, whereupon $T_{(0,0,0)}X = k^3$. The rank of J_p is either 0 or 1, and solving the equations shows that if $\lambda^3 \neq 27$ then the only point p where $T_pX = k^3$ is $p = (0,0,0)$. Elsewhere, $T_pX \simeq k^2$ (which correspond to the "smooth points" of X). The other points are called "singular".

Consider the cyclic group of order 3, where $G = (\xi, 0; 0, \xi^{-1})$ acts on $\mathbb{C}^2$ by left multiplication. We defined $\mathbb{C}^2/G$ in terms of its coordinate ring; so we can ask where it's singular.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 20: May 19

Why valuations?

The Hasse principle.

If $f \in \mathbb{Z}[x,y,z]$ is homogeneous, then $f(\lambda x, \lambda y, \lambda z) = \lambda^d f(x,y,z)$ where $d = \deg f$. Then we ask if there are (non-trivial) solutions to $f(x,y,z) = 0$ in $\mathbb{Q}^3$. Then there is a solution in $(\lambda x, \lambda y, \lambda z) \in \mathbb{Z}^3$, as well as a solution in F_p.

Notice that questions about affine varieties can be recovered from questions about projective varities (using a suitable embedding); so there is no harm restricting to homogeneous.

If there is a prime p such that $f(x,y,z)$ has no non-trivial solutions in $\mathbb{Z}_p$, then there is no non-trivial solution in $\mathbb{Q}$. The Hasse principal consists of theorems that provide a partial converse.

Now you can look at solutions in $\mathbb{Z}/p^r$, and taking inverse limits leads to

$$\lim_{\leftarrow}\left(\frac{\mathbb{Z}}{p^n}\right) \simeq \mathbb{Z}_p \subset \mathbb{Q}_p.$$

$\mathbb{Z}_p$ is called the p-adic integers. You can put a norm $d_p(x,y) = \nu_p(x-y)$ on $\mathbb{Q}_p$, and it is nicer than $\mathbb{Q}$ (because it has a better topology).

From the point of view of algebraic geometry, you don't want to separate the geometry from the arithmetic (and the construction of $\mathbb{Q}_p$ was a purely arithmetic process).

Putting in the geometry

Let C be an irreducible affine algebraic curve. For each point $p \in C$, there is a valuation ν_p. In the homework, we were looking at

$$\cdots \subset \mathfrak{m}_p^2 \subset \mathfrak{m}_p \subset \mathcal{O}(C) \subset \mathfrak{m}_p^{-1} \subset \cdots \subset \operatorname{Frac}\mathcal{O}(C)$$

where $\mathfrak{m}_p^{-1}$ is a fractional ideal. If p is a smooth point, then $\mathfrak{m}_p \cdot \mathfrak{m}_p^{-1} = \mathcal{O}(C)$. What you're doing is counting the zeroes and the poles (when you're working with all the valuations, so we're getting the information about zeros and poles). Essentially, this extends the setup of complex analysis. You can have elements in $\operatorname{Frac}\mathcal{O}(C)$ not in any of the $\mathfrak{m}_p^{-n}$; for instance, $1/(x-2)$ in $k(x)$ or $1/5$ when $p = 3$.

Back to Tangent Spaces

Recall that for $X \subset \mathbb{A}^n$,

$$L_q = \{p + \lambda q : \lambda \in k\}.$$

Then we defined

$$T_pX = \{q \in k^n : L_q \text{ tangent to } X \text{ at } p\} = \ker(J_p : k^n \to k^m)$$

where the Jacobian matrix $J_p = \left(\frac{\partial f_i}{\partial x_j}(p)\right)$.

From calculus, we know that tangent spaces are local data, so we would like to realize them as such.

Remark. V is a finite dimensional vector space, and $D \subset V^*$ is a subspace. Consider an s.e.s.

$$0 \to D \to V^* \to V^*/D \to 0.$$

Applying $\mathrm{Hom}_k(\_, k)$, we obtain the s.e.s.

$$0 \to (V^*/D)^* \to V \to D^* \to 0.$$

We are using the fact that the function $V \to V^{**}$ is naturally isomorphic to the identity.

Definition 20.1. The **orthogonal complement** is defined to be $D^\perp = (V^*/D)^*$.

Theorem 20.2. *If $p \in X$ and $\mathfrak{m}_p$ is the maximal ideal in $\mathcal{O}(X)$ vanishing at p, then there is a vector space isomorphism*

$$d_p : \mathfrak{m}/\mathfrak{m}^2 \to (T_pX)^*.$$

Proof. Let $x_1, \cdots, x_n$ be coordinate functions on K^n. Write $p = (\alpha_1, \cdots, \alpha_n)$. Then $\mathfrak{n} = (x_1 - \alpha_1, \cdots, x_n - \alpha_n) \subset k[x_1, \cdots, x_n]$. Since $\mathcal{O}(X) = \mathcal{O}(\mathbb{A}^n)/I(X)$,

$$\mathfrak{m}_p = \frac{\mathfrak{n} + I(X)}{I(X)} = \frac{\mathfrak{n}}{I(X)}.$$

Observe that $\mathfrak{m}_p^2 = \frac{\mathfrak{n}^2 + I(X)}{I(X)}$ (from the definition of coset multiplication), so that

$$\frac{\mathfrak{m}_p}{\mathfrak{m}_p^2} = \frac{\mathfrak{n}/I(X)}{(\mathfrak{n}^2 + I(X))/I(X)} \simeq \frac{\mathfrak{n}}{\mathfrak{n}^2 + I(X)},$$

by the third isomorphism theorem.

Define $\psi : \mathfrak{n} \to (k^n)^*$ by $\psi(f) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p) x_i$. Since the $x_i \in (k^n)^*$, this makes sense. Now $\psi(x_i - \alpha_i) = x_i$ (which form a basis), so ψ is surjective. Also notice that $\psi(\mathfrak{n}^2) = 0$ because of the product rule. Since $\dim \mathfrak{n}/\mathfrak{n}^2$, we can translate everything back to the origin and we are looking at $(x_1, \cdots, x_n)/(x_1, \cdots, x_n)^2$. Thus it has dimension n. Thus ψ induces an isomorphism from $\mathfrak{n}/\mathfrak{n}^2 \to (k^n)^*$.

Let $q = (\lambda_1, \cdots, \lambda_n)$. Then $\psi(f)(q) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p)\lambda_i$. Hence $T_pX = \ker J_p$.

Recall $I(X) = (f_1, \cdots, f_n)$. Now $\psi(I(X))(q) = 0$ precisely when $q \in \psi(I(X))^\perp$. Thus

$$T_p X = \left(\frac{n^2 + I(X)}{n^2}\right)^\perp = \left(\frac{n}{n^2 + I(X)}\right)^* .$$

Now after a little bit of work, we see that this is $(m_p/m_p^2)^*$, and the result follows. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 21: May 23

Dimension

Recall that $\dim T_pX = \dim_k(\mathfrak{m}_p/\mathfrak{m}_p^2)$, and for X irreducible we define

$$\dim X = \min\{\dim T_pX : p \in X\}.$$

We want to check that the dimension behaves as it should. To compute $\dim \mathbb{A}^n$, we work in $k[x_1, \cdots, x_n]$. Without loss of generality, any maximal ideal (up to translation) is

$$\mathfrak{m} = (x_1, \cdots, x_n).$$

Then $\{x_1, \cdots, x_n\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$ so $\dim T_p\mathbb{A}^n = n$ and therefore $\dim \mathbb{A}^n = n$.

A single point has dimension 0, since $k/k^2 = 0$. It turns out that the empty set has dimension -1.

Definition 21.1. A **hypersurface of** $\mathbb{A}^n$ is a set $X = V(f)$ where $f \in k[x_1, \cdots, x_n] \setminus k$.

Theorem 21.2. *The dimension of a hypersurface is* $n - 1$.

Proof. To show that the dimension is not less than $n - 1$, consider

$$\mathfrak{m}_p = (x_1, \cdots, x_n) \subset k[x_1, \cdots, x_n].$$

Now if the dimension was n, then by definition $\dim T_pX = n$ for all $p \in X$. Hence

$$J_p = \left(\tfrac{\partial f}{\partial x_1}(p), \cdots, \tfrac{\partial f}{\partial x_n}(p)\right)$$

has rank 0 for all $p \in X$.

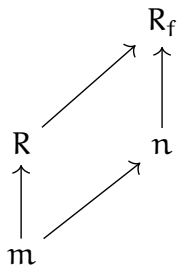
Consequently $\left(\frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right) \subset (f)$. But $\deg_{x_i}(\partial_{x_i} f) < \deg_{x_i}(f)$, so the only way for any $\partial_{x_i} f$ to be a multiple of f is for $\partial_{x_i} f = 0$. When $\mathrm{char}(k) = 0$, this implies f is constant (contradiction).

If $\mathrm{char}(k) = p > 0$, then we get $f \in k[x_1^p, \cdots, x_n^p]$. Then $f = g^p$, contradicting irreducibility. □

The tangent space is "local"; it doesn't change when you restrict to an open set (well, as long as your open set is a variety; we don't know how to talk about other things yet). So consider $X_f = X \setminus V(f)$.

Proposition 21.3. *For* $p \in X_f$, $\dim T_pX = \dim T_pX_f$.

Proof. Write $R = \mathcal{O}(X)$ and $R_f = \mathcal{O}(X_f) = \mathcal{O}(X)[f^{-1}]$. Let $\mathfrak{m}, \mathfrak{n}$ be the maximal ideals at p in R, R_f. We must show that $\dim(\mathfrak{m}/\mathfrak{m}^2) = \dim(\mathfrak{n}/\mathfrak{n}^2)$.



It suffices to show that $\mathfrak{m} \to \mathfrak{n} \to \mathfrak{n}/\mathfrak{n}^2$ is surjective with kernel $\mathfrak{m}^2$; this amounts to showing $\mathfrak{n} = \mathfrak{m} + \mathfrak{n}^2$ (surjectivity) and $\mathfrak{m}^2 = \mathfrak{m} \cap \mathfrak{n}^2$ (kernel = $\mathfrak{m}^2$). Since $\mathfrak{m} = R \cap \mathfrak{n}$, it follows that $\mathfrak{m} \cap \mathfrak{n}^2 = R \cap \mathfrak{n}^2$.

Consider $af^{-r} \in \mathfrak{n}$ for $a \in R$. Since af^{-r} vanishes at p, $a(p) = 0$. Hence

$$\mathfrak{n} \subset \mathfrak{m}R_f \subset \mathfrak{n}R_f = \mathfrak{n} \implies \mathfrak{n} = \mathfrak{m}R_f.$$

To show that $\mathfrak{n} = \mathfrak{m} + \mathfrak{n}^2$, it suffices to show that $\mathfrak{n} \subset \mathfrak{m} + \mathfrak{n}^2$. Let $a \in \mathfrak{m}$, so $af^{-r} \in \mathfrak{n}$. Then $1 - f(p)^{-n}f^n \in \mathfrak{m}$ since it vanishes at p. Now look at $a(1 - f(p)^{-n}f^n)f^{-n} \in \mathfrak{n}^2$. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 22: May 28

Dedekind Domains

We will discuss the properties of Dedekind domains, then we will define them.

1. If K is a number field, the ring of integers $\mathcal{O}_K$ is a Dedekind domain.

   Definition 22.1. A **number field** is a finite extension of $\mathbb{Q}$.

   Definition 22.2. The **ring of integers** $\mathcal{O}_K$ of a number field is the integral closure of $\mathbb{Z}$ in K.

   The relationship between $\mathcal{O}_K$ and K is the same as that of $\mathbb{Z}$ and $\mathbb{Q}$.

2. If X is a smooth irreducible curve, then $\mathcal{O}(X)$ is a Dedekind domain.

   Definition 22.3. A **curve** X is an affine algebraic variety such that $\dim T_p X = 1$ for all $p \in X$.

Note that PIDs are Dedekind domains, and their structure reflects that of PIDs and their modules:

Differences: Dedekind domains have non-free projective modules.

Similarities: Let R be a Dedekind domain. Every ideal in R is generated by "almost" one element and is projective. There is a structure theorem for finitely generated R-modules M:

$$M = \left(\bigoplus R/\mathfrak{m}_j^{n_j}\right) \oplus (I_1 \oplus \cdots \oplus I_n) \text{ for some ideals } I_j \subset R,\ \mathfrak{m}_j \text{ maximal.}$$

The first term is the torsion submodule, and the second is torsion-free.

Theorem 22.4. *Non-zero ideals in a Dedekind domain factor as a product of maximal ideals.*

For the rest of today, R is a (commutative, unital) noetherian domain, with field of fractions $K \neq R$.

Definition 22.5. R is called a Dedekind doman if is **integrally closed** in K and has **Krull dimension 1**; in other words, every non-zero prime ideal is maximal.

Equivalent definitions:

(a) Every non-zero (proper) ideal factors into primes

(b) The monoid of fractional ideals is a group

(c) R is noetherian and the localization at each maximal ideal is a DVR

Fractional Ideals

There is a fruitful analogy between R, K and $\mathbb{Z}, \mathbb{Q}$; thus we think of ideals in R as "idealized numbers". Let M be an R-module that is a submodule of K.

Definition 22.6. M is called a **fractional ideal** if $xM \subset R$ for some $0 \neq x \in R$.

Note that xM is an ideal in R that is isomorphic to M as an R-module. Also fractional ideals are finitely generated R-modules, and every ideal in R is a fractional ideal (with $x = 1$).

If M, N are fractional ideals, then so is the product ideal MN. In fact, the set of fractional ideals form an abelian monoidal structure, under the operation of ideal multiplication.

Proposition 22.7. *The set of fractional ideals is a group under ideal multiplication.*

Proof. Define

$$M^{-1} = \{x \in K : xM \subset R\}.$$

It is not hard to see that M^{-1} is an R-submodule of K. It's non-zero, since M is a fractional ideal. It's a fractional ideal since $yM^{-1} \subset R$ for all $y \in M$. It suffices to show that $MM^{-1} = R$.

We prove this result for maximal ideals $\mathfrak{m}$. So consider $x \in \mathfrak{m} \setminus \{0\}$. Since R is noetherian, there are primes $p_1, \cdots, p_n$ such that $p_1 \cdots p_n \subset xR$. Choose n minimal with respect to this property. Since $xR \subset \mathfrak{m}$, we may assume without loss of generalitythat $p_j = \mathfrak{m}$. Then $x^{-1}p_2 \cdots p_n \subset \mathfrak{m}^{-1}$, so by minimality $x^{-1}p_2 \cdots p_n \notin R$.

Consequently $\mathfrak{m}^{-1} \supsetneq R$. Then $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1} \subset R$. If $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$, then $\mathfrak{m}(\mathfrak{m}^{-1})^2 = \mathfrak{m}$ so $(\mathfrak{m}^{-1})^2 \subset \mathfrak{m}^{-1}$. It follows that $\mathfrak{m}^{-1}$ is a ring containing R; but it's a finite extension of an integrally closed ring, and is therefore integrally closed. Consequently $\mathfrak{m}^{-1} = R$, which is a contradiction. Hence $\mathfrak{m}\mathfrak{m}^{-1} = R$ as desired. □

Theorem 22.8 (Unique Factorization)**.** *Every non-zero ideal in a Dedekind domain is a product of maximal ideals; this decomposition is unique.*

Proof. Since R is noetherian, we may choose an ideal I that is maximal with respect to"not being a product of maximal ideals". Let $\mathfrak{m}$ be a maximal ideal containing I. Since I is not maximal, $\mathfrak{m} \neq I$. Then $I\mathfrak{m}^{-1}$ is an ideal containing I. If $I\mathfrak{m}^{-1} \neq I$ would be a product of maximal ideals (by maximality of I). Consequently $I = \mathfrak{m}p_1 \cdots p_n$, whereupon $I\mathfrak{m}^{-1} = I$.

Set $S = \bigcup_{n=1}^{\infty} (\mathfrak{m}^{-1})^n$; it follows that S is a ring containing R. Since $\mathfrak{m}^{-1} \supsetneq R$, it follows that $S \neq R$. We will continue the proof next time. □

Math 506 Modern Algebra Notes by Avi Levy

Lecture 23: May 30

Open problem: Do there exist infinitely many square-free positive integers d such that

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \overline{\mathbb{Z}}, \text{ (where } \mathbb{Z} \subset \mathbb{Q}[\sqrt{d}])$$

is a PID? Note that $\mathcal{O}_K$ is always a Dedekind domain.

The standard example of a Dedekind domain that is not a PID is $\mathbb{Z}[\sqrt{-5}]$, and another nice one is

$$A = \frac{\mathbb{R}[x,y]}{(x^2+y^2-1)}$$

which is a Dedekind domain that is not a PID. To prove it's a Dedekind domain, the tricky step is integrally closed. Start by extending to the complex; then

$$\mathbb{C} \otimes_{\mathbb{R}} A = \frac{\mathbb{C}[x,y]}{(x^2+y^2-1)} \simeq \mathbb{C}[u,u^{-1}],$$

where $u = x + iy$, so $u^{-1} = x - iy$ (since $x^2 + y^2 = 1$ after modding out). To show it's not a PID, take a maximal ideal like $m = (x, y-1)$. It is not principal.

In fact, a maximal ideal m is principal precisely when $A/m \simeq \mathbb{C}$. Look at

$$\begin{aligned} m^2 &= (x^2, x(y-1), (y-1)^2) \\ &= (1-y^2, x(y-1), y^2-2y+1) \\ &= (1-y^2, x(y-1), -2y+2) \\ &= (y-1). \end{aligned}$$

Lastly, all non-principal ideals in A are isomorphic.

Projective modules are the algebraist's vector bundle. In a Dedekind domain, we will prove that every ideal is projective; so we may ask what bundle $(x, y-1)$ corresponds to. It turns out to be the Möbius bundle.

$$\begin{array}{ccc} M & \hookrightarrow & \mathbb{R}^4 \\ {\scriptstyle \mathbb{R}}\downarrow & \nearrow_{s} & \\ S^1 & & \end{array}$$

We look at the module of continuous algebraic sections, $\Gamma(M)$. To be an algebraic section, it has to be an algebraic subvariety (the total space of M is cut out by polynomial equations). Then for any $f \in A$, we have

$$(fs)(p) = f(p)s(p) \in \Gamma(M), \text{ for } s \in \Gamma(M)$$

We end up obtaining $\Gamma(M) \simeq \mathfrak{m}$, which reflects the non-trivial bundle structure. On the other hand, $\mathfrak{m} \otimes_A \mathfrak{m} \simeq A$. But we obtain

$$\mathfrak{m} \otimes_A \mathfrak{m} \simeq \mathfrak{m} \otimes_A \mathfrak{m}^{-1} \simeq \mathfrak{m}\mathfrak{m}^{-1} = A.$$

Moreover $\mathfrak{m} \oplus \mathfrak{m} \simeq A^2$. Thus we have shown a statement about the class group K_0 of real vector bundles.

Back to the proof from last time

We had $I \neq 0$ maximal such that I is not a product of maximal ideals. Then $I \subset \mathfrak{m}$ and $I\mathfrak{m}^{-1} = I$. We were considering

$$R \subset S = \bigcup_{n=1}^{\infty} (\mathfrak{m}^{-1})^n.$$

Observe that $SI = I$ (from $I\mathfrak{m}^{-1} = I$). If $x \in I \setminus \{0\}$, then xS is an ideal of R, and hence finitely generated as an R-module. But $xS \simeq S$ as an R-module (the map $s \mapsto xs$ is an S-module homomorphism). Hence S is a finitely generated R-module, so it is integral over R. By integral closure, $S = R$, whereupon we obtain the contradiction $\mathfrak{m}^{-1} \subset R$. Hence no such I exists, which means every non-zero ideal in R is a product of maximal ideals.

It remains to prove uniqueness; suppose that $\mathfrak{m}_1 \cdots \mathfrak{m}_k = \mathfrak{n}_1 \cdots \mathfrak{n}_l$ where all $\mathfrak{m}_i, \mathfrak{n}_j$ are maximal. Then

$$\mathfrak{n}_1 \cdots \mathfrak{n}_l \subset \mathfrak{m}_1,$$

but by primality we have $\mathfrak{n}_j \subset \mathfrak{m}_1$ for some j; by maximality, $\mathfrak{n}_j = \mathfrak{m}_1$. Relabel such that $j = 1$; then we obtain

$$\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k = \mathfrak{m}_1 \mathfrak{n}_2 \cdots \mathfrak{n}_l,$$

so we left-multiply by $\mathfrak{m}_1^{-1}$ to obtain $\mathfrak{m}_2 \cdots \mathfrak{m}_k = \mathfrak{n}_2 \cdots \mathfrak{n}_l$ (using $\mathfrak{m}_1 \mathfrak{m}_1^{-1} = R$). Uniqueness follows by induction.

Corollary 23.1. *Every fractional ideal over a Dedekind domain is invertible.*

Proof. Let M be a fractional ideal for a Dedekind domain R. Then $xM \subset R$ for some $0 \neq x \in R$. Now

$$xM = \mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_n \implies M = x^{-1} \mathfrak{m}_1 \cdots \mathfrak{m}_k.$$

Expanding MM^{-1}, we find

$$MM^{-1} = (x^{-1} \mathfrak{m}_1 \cdots \mathfrak{m}_k)(x \mathfrak{m}_1^{-1} \cdots \mathfrak{m}_k^{-1}) = R.$$

□

The class group of a Dedekind domain

The set of fractional ideals is an abelian group, G, under the multiplication $M \times N = MN$, with R as the identity. The set

$$H = \{xR : 0 \neq x \in K\}$$

is a subgroup of G.

Definition 23.2. The **class group** of R, denote by $\mathrm{Cl}(R)$, is G/H.

For algebraic geometers, this is a special case of the Picard group.

If R is the ring of integers in a number field K, call $\mathrm{Cl}(R)$ the **class group** of K, and

$$h = |\mathrm{Cl}(R)| < \infty$$

in this case.

Definition 23.3. The **class number** of K is the integer h defined above.

Consider the case

$$R = \frac{\mathbb{C}[x,y]}{(y^2 - x(x-1)(x-\lambda))}, \qquad \lambda \neq 0, 1.$$

Then R is a Dedekind domain and $\mathrm{Cl}(R)$ is uncountable (so the finiteness for number fields is very special).

It is known that for all $h \geq 1$, there are only finitely many imaginary quadratic fields with class number h. However, it is unknown how many real quadratic fields there are with class number h.

Elliptic curves live in the projective plane, so we take the closure of the R we have written down. This involves adding a point at infinity, and now we should think of the elliptic curve like a torus. But a torus is isomorphic to $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, which is an abelian group. You can choose any point on the elliptic curve to be the identity, but the group law is particularly elegant if you choose the point at infinity. The group law says that to add two points, you take the secant through those points and look at the the third. This gives you points of 2-torsion, which correspond in the lattice picture. Thus we get $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the subgroup of 2-torsion points, and similarly the n-torsion points form the subgroup $\mathbb{Z}_n \times \mathbb{Z}_n$.

Definition 23.4. A prime p is called **irregular** if p divides the class number of $\mathbb{Q}(e^{2\pi i/p})$.

Kummer proved that Fermat's Last Theorem holds for regular primes. It is known that 61% of primes below 163×10^6 are regular.

Math 506 Modern Algebra Notes by Avi Levy

Lecture 24: June 6

Proposition 24.1. *Every UFD is integrally closed.*

Proof. Let R be a UFD with $K = \operatorname{Frac} R$. Suppose that a/b is integral over R, where $a, b \in R$. Cancelling common factors of a, b, we can assume that $\gcd(a, b) = 1$. Then we have

$$\left(\frac{a}{b}\right)^n + \alpha_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + \alpha_1\left(\frac{a}{b}\right)\alpha_0 = 0,$$

whereupon multiplying by b^n yields $a^n + bc = 0$ for some $c \in R$. Then $b \mid a^n$, so since $\gcd(a, b) = 1$ we have b is a unit and $a/b \in R$. □

Finishing a proof from last time: Every finitely generated torsion-free R-module (where R is a Ded. domain) is projective and isomorphic to a direct sum of ideals. So far, we showed that such a module is isomorphic to a submodule of R^n for some n.

Let $I \subset R$ be an ideal. Then $II^{-1} = R$. If $I = aR + \cdots + a_nR$, then write

$$1 = a_1b_1 + \cdots + a_nb_n$$

with all $b_i \in I^{-1}$. Consider the maps

$$\begin{aligned} \alpha &: R^n \to I, & (r_1, \cdots, r_n) &\mapsto a_1r_1 + \cdots + a_nr_n \\ \beta &: I \to R^n, & a &\mapsto (ab_1, \cdots, ab_n). \end{aligned}$$

Then $\beta\alpha = \mathrm{Id}_I$, so therefore I is projective due to the short exact sequence

$$0 \longrightarrow \ker\beta \xrightarrow{\beta} R \xrightarrow{\alpha} I \longrightarrow 0.$$

By the lemma, every submodule of a finitely generated free module is projective. Actually, the proof showed a bit more:

$$0 \longrightarrow M \cap \ker\pi \longrightarrow M \longrightarrow \pi(M) \longrightarrow 0$$

was exact. Hence $M \simeq \ker\pi \cap M \oplus \pi(M)$ is a direct sum with an ideal. By induction, it follows that M is a direct sum of ideals. □

Corollary 24.2. *If M is a finitely generated R module where R is a Ded. domain, then $M \simeq \tau M \oplus (M/\tau M)$.*

Proof. Look at the s.e.s.

$$0 \longrightarrow \tau M \longrightarrow M \longrightarrow M/\tau M \longrightarrow 0$$

Since $M/\tau M$ is finitely generated and torsion-free, it is projective and therefore the sequence splits. □

Lemma 24.3. *Let $\mathfrak{m}$ be a maximal ideal in a Ded. domain R, and M a finitely generated R-module such that $\mathfrak{m}^n M = 0$ but $\mathfrak{m}^{n-1} M \neq 0$. Then $M \simeq R/\mathfrak{m}^n \oplus M'$.*

Proof. By hypothesis, there is an $x \in M$ such that $\mathfrak{m}^n x = 0$ but $\mathfrak{m}^{n-1} x \neq 0$. Hence $Rx \simeq R/\mathfrak{m}^n$. Since the only ideals in $R/\mathfrak{m}^n$ are the images of $R \supset \mathfrak{m} \supset \cdots \supset \mathfrak{m}^n$, it follows that $R/\mathfrak{m}^n$ is injective over itself. Hence $Rx \subset M$ is injective and therefore $M \simeq Rx \oplus M'$ for some submodule $M' \subset M$. □

Proposition 24.4. *If M is a finitely generated torsion module over a Ded. domain R, then*

$$M \simeq R/\mathfrak{m}_1^{n_1} \oplus \cdots \oplus R/\mathfrak{m}_k^{n_k}$$

for some maximal ideals $\mathfrak{m}_j$ and $n_j \in \mathbb{N}$.

Proof. Let $M = m_1 R + \cdots + m_t R$. Let $r_i \in R$ be nonzero such that $r_i m_i = 0$. Then the ideal

$$I = r_1 \cdots r_t T$$

annihilates M. Since $I = p_1^{j_1} \cdots p_s^{j_s}$ for some pairwise distinct maximal ideals p_k, it follows that

$$\frac{R}{I} \simeq \frac{R}{p_1^{j_1}} \oplus \cdots \oplus \frac{R}{p_s^{j_s}}.$$

Writing $1 = e_1 + \cdots + e_n$ where the e_i are orthogonal idempotents, we have $M = M_1 \oplus \cdots \oplus M_s$ where $M_i = e_i M$. Each M_i is an $R/p_i^{j_i}$ module, and let l_i be the smallest integer such that $p_i^{l_i} M_i = 0$. By the lemma,

$$M_i \simeq \frac{R}{p_i^{l_i}} \oplus M_i'$$

and repeat. Since R has finite length, so does M. Then each M_i has finitely length, as do its quotients. Thus the process terminates.

Another way to see this: we proved that if I is an ideal in a Ded. domain, then R/I has finite length. Then M as an R/I module has finite length. □

Proposition 24.5. *Let I, J be fractional ideals over a Ded. domain R.*

1. *There is a fractional ideal M such that $I \oplus J \simeq R \oplus M$.*
2. *M is unique up to R-module isomorphism.*
3. *If M, N are fractional ideals such that $M \oplus R \simeq N \oplus R$, then $M \simeq N$.*

Corollary 24.6. *If P is a finitely generated projective R-module, then $P \simeq R^n \oplus I$ for some ideal I that is unique up to isomorphism of R-modules.*

Proof. Apply the proposition repeatedly, and use the fact that fractional ideals are isomorphic to ideals. □

Definition 24.7. If M is an R-module, define $M^* = \mathrm{Hom}_R(M, R)$.

Aside: When M is a finitely generated projective left A-module, then $M \to M^{**}$ is an isomorphism.

Proof of the proposition. If M is a fractional ideal, then $M^* \simeq M^{-1}$. Indeed, consider the map

$$\Phi : M^{-1} \to M^*, \qquad \Phi(x)(m) = xm.$$

On the other hand, consider $\alpha : M \to R$. Then without loss of generality, $M \supset R$. Let $q = \alpha(1)$; then for any $m \in R$, we have

$$\begin{aligned} \alpha(m) &= \alpha(m1) \\ &= m\alpha(1) = qm. \end{aligned}$$

If $m' \in M$, there is an $x \in R$ such that $xm' \in R$, so $x\alpha(m') = \alpha(xm') = qxm'$. Cancelling yields $\alpha(m') = qm'$. Hence $q \in M^{-1}$ and $\alpha(m') = \Phi(q)(m')$ whereupon $\alpha = \Phi(q)$.

There is an injective R-module homomorphism

$$R \hookrightarrow I^* \oplus J^*, \qquad 1 \mapsto (\alpha, \beta).$$

Apply $\mathrm{Hom}_R(\_, R)$ to this, which yields

$$(I^* \oplus J^*)^* \to R^*.$$

Hence we get $I \oplus J \to R$ (up to isomorphism), where the maps are onto. □