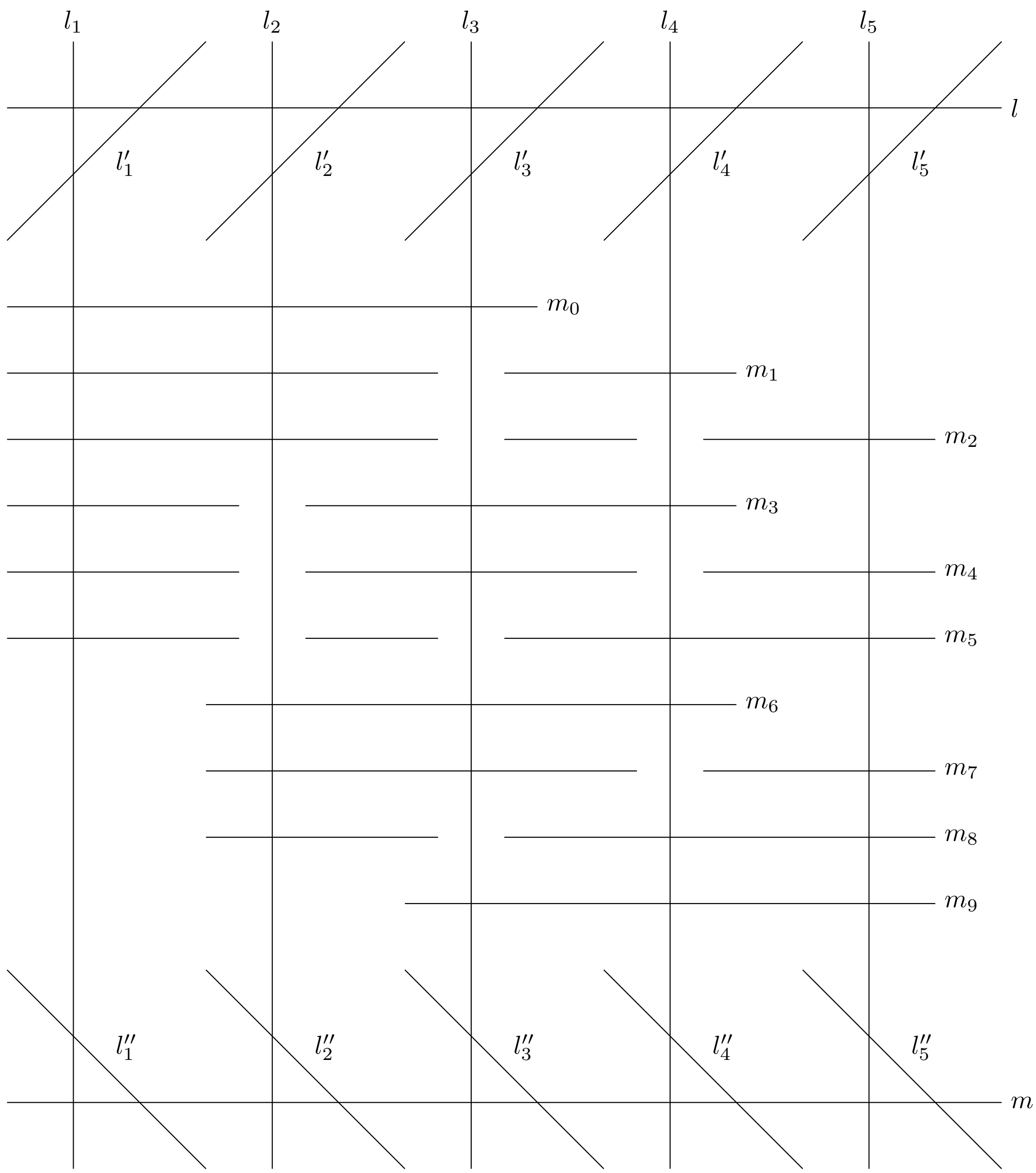
M4P33 Algebraic Geometry

Lectured by Dr Genival Da Silva Jr
Typed by David Kurniadi Angdinata

Spring 2019



Syllabus

Affine varieties. Projective varieties. Morphisms. Rational maps. Nonsingular varieties. Intersections in projective space. The 27 lines on a cubic surface. Grassmannians. Divisors on curves. Elliptic curves.

Contents

0 Introduction

Lecture 1 Friday 11/01/19

I will not follow a particular book, but everything I am going to say will be contained in one of the following books.

- I Shafarevich, Basic algebraic geometry, 1974
- R Hartshorne, Algebraic geometry, 1977
- J Harris, Algebraic geometry: a first course, 1922
- M Reid, Undergraduate algebraic geometry, 1988

1 Affine varieties

Notation 1.1.

- R is a commutative ring with unity.
- K is a field.
- $K[x_1, \ldots, x_n]$ is the ring of polynomials in n variables.
- $\mathbb{A}^n$ is K^n as a set.

Definition 1.2. Let $S \subseteq K[x_1, \ldots, x_n]$ then

$$Z(S) = \{x \in \mathbb{A}^n \mid \forall f \in S,\ f(x) = 0\}$$

is called the **zero locus** of S. Subsets of $\mathbb{A}^n$ that are of this form are called **affine varieties**.

Remark 1.3. Some authors call **algebraic set** the object $Z(S)$. We will not follow this notation.

Example 1.4.

- Single points $p = (p_1, \ldots, p_n)$. $p = Z(S)$ where $S = \{x_1 - p_1, \ldots, x_n - p_n\}$.
- $\mathbb{A}^n = Z(0)$.
- $\emptyset = Z(1)$.
- Subspaces of $\mathbb{A}^n = K^n$.
- If $X = Z(f_1, \ldots, f_n) \subseteq \mathbb{A}^n$ and $Y = Z(g_1, \ldots, g_m) \subseteq \mathbb{A}^n$ are affine varieties then

  $$X \times Y = Z(f_1, \ldots, f_n, g_1, \ldots, g_m) \subseteq \mathbb{A}^{n+m}$$

  is a variety.

Remark 1.5. If $S \subseteq K[x_1, \ldots, x_n]$ and $I = \langle S \rangle$ then $Z(S) = Z(I)$.

Theorem 1.6 (Hilbert's basis theorem)**.** *If R is Noetherian then $R[x]$ is Noetherian.*

Corollary 1.7. *Every ideal in $K[x_1, \ldots, x_n]$ is finitely generated.*

Definition 1.8. Let $X \subseteq \mathbb{A}^n$ then

$$I(X) = \{f \in K[x_1, \ldots, x_n] \mid \forall x \in X,\ f(x) = 0\}.$$

Example 1.9. $I(p) = I((p_1, \ldots, p_n)) = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$.

Goal is

$$\begin{array}{rcl} \{\text{affine varieties in } \mathbb{A}^n\} & \leftrightarrow & \{\text{ideals of } K[x_1, \ldots, x_n]\} \\ X & \mapsto & I(X) \\ Z(J) & \leftarrow\!\shortmid & J \end{array}.$$

$Z(I(X)) = X$ but $I(Z(J)) \supseteq J$.

Example 1.10. $J = \left\langle x^2 + 1 \right\rangle \subseteq \mathbb{R}[x] = I(\emptyset) = I\left(Z\left(x^2 + 1\right)\right)$.

Proposition 1.11.

- *If $X \subseteq Y$ then $I(Y) \subseteq I(X)$. If $I \subseteq J$ then $Z(J) \subseteq Z(I)$.*
- *$X \subseteq Z(I(X))$ and $S \subseteq I(Z(S))$.*
- *If X is affine then $Z(J(X)) = X$. If $X = Z(S)$ then take Z of $S \subseteq I(Z(S))$.*

Example 1.12. Let $J \subseteq \mathbb{C}[x]$. $J = \langle f \rangle$, where $f = (x - x_1)^{k_1} \dots (x - x_n)^{k_n}$.

Definition 1.13. Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal.

$$I \subseteq \sqrt{I} = \{f \in K[x_1, \dots, x_n] \mid \exists n \in \mathbb{N},\ f^n \in I\}.$$

If $\sqrt{I} = I$, we say I is a **radical ideal**. (Exercise: $\sqrt{I}$ is an ideal, $I \subseteq \sqrt{I}$, and $\sqrt{I} = \bigcap_{p \text{ prime}} p$)

Theorem 1.14 (Hilbert's Nullstellensatz)**.** *$I(Z(J)) = \sqrt{J}$. If $\sqrt{J} = J$ then*

$$\begin{array}{rcl} \{\textit{affine varieties}\} & \leftrightarrow & \{\textit{radical ideals}\} \\ X & \mapsto & I(X) \\ Z(J) & \leftarrow\!\shortmid & J \end{array}.$$

Lecture 2 Monday 14/01/19

Proposition 1.15.

1. *$Z(S) \cup Z(T) = Z(ST)$.*
2. *$\bigcap_i Z(S_i) = Z(\bigcup_i S_i)$.*
3. *$Z(0) = \mathbb{A}^n$ and $Z(1) = \emptyset$.*

Proof.

1. If $p \in Z(S) \cup Z(T)$, then $f(p) = 0$ for $f \in S$ or $f \in T$, so $f(x) = 0$ for $f \in ST$, where

$$ST = \left\{ \sum_{i \in I,\ I \text{ finite}} s_i t_i \right\} \subseteq S \cap T,$$

with equality if $S + T = R$. If $p \in Z(ST)$, there exists f such that $f(p) = 0$ for $f \in S$ or $f(p) = 0$ for $f \in T$, so $p \in Z(S) \cup Z(T)$.

□

Definition 1.16. The **Zariski topology** on $\mathbb{A}^n$ is the topology generated by closed sets of the form $Z(S)$. By the above proposition this is a topology.

Example 1.17. $\mathbb{A}^1$ is not Hausdorff.

Definition 1.18. A topological space X is **irreducible** if it cannot be expressed as a union $X = A \cup B$, where A and B are proper and closed subsets. $\emptyset$ is not considered irreducible.

Example 1.19. $\mathbb{A}^1$.

Example 1.20. Any non-empty open set of irreducible X is dense and irreducible. Suppose A is open then $X = A^c \cup \overline{A}$. Since X is irreducible then $A^c = X$, a contradiction, or $\overline{A} = X$. Suppose A is reducible. Let $A = (A \cap B) \cup (A \cap C)$, where B and C are closed. Then $X = A^c \cup (B \cup C)$. $A^c = X$ or $B \cup C = X$, which are contradictions.

Example 1.21. If A is irreducible then $\overline{A}$ is also irreducible. Suppose $\overline{A}$ is not irreducible. $\overline{A} = \left(\overline{A} \cap B\right) \cup \left(\overline{A} \cap C\right)$. Take $\bigcap A$, $A = (A \cap B) \cup (A \cap C)$, a contradiction.

Definition 1.22. An affine variety is **irreducible** if it is irreducible as a topological space.

Remark 1.23. A **quasi-affine variety** is an open set of an affine variety.

Proposition 1.24.

1. *$I(X \cup Y) = I(X) \cap I(Y)$.*
2. *$Z(I(X)) = \overline{X}$ for any $X \subseteq \mathbb{A}^n$.*

Proof.

1. If $f \in I(X \cup Y)$ then $f(p) = 0$ for all $p \in X \cup Y$, so $f \in I(X)$ and $f \in I(Y)$.
2. We know that $X \subseteq Z(I(X))$ hence $\overline{X} \subseteq Z(I(X))$. Now, let Y be a closed set containing X, that is $X \subseteq Y$. Then
$$I(Y) \subset I(X) \qquad \implies \qquad Z(I(X)) \subset Z(I(X)) = Y,$$
so any closed set containing Y contains $Z(I(X))$.

□

Proposition 1.25. *X is irreducible if and only if $I(X)$ is prime.*

Proof.

$\implies$ Let $f, g \in I(X)$.
$$X \subseteq Z(fg) = Z(f) \cup Z(g) \qquad \implies \qquad X = (X \cap Z(f)) \cup (X \cap Z(g)).$$
$Z(f) \subseteq X$, so $f \in I(X)$, or $Z(g) \subseteq X$, so $g \in I(X)$.

$\impliedby$ Exercise.

□

Example 1.26. $\mathbb{A}^n$.

Definition 1.27. If $X \subseteq \mathbb{A}^n$, the **coordinate ring** of X is
$$A(X) = \frac{A}{I(X)} = \frac{K[x_1, \dots, x_n]}{I(X)}.$$

Lecture 3 Tuesday 15/01/19

Example 1.28. Let $f \in K[x_1, \dots, x_n]$ be irreducible. If $n = 3$, $Z(f)$ is a surface. If $n = 2$, $Z(f)$ is a curve.

Example 1.29. Let $y - x^2 \in K[x, y]$. Then
$$\begin{array}{ccc} A(X) = \dfrac{K[x,y]}{\langle y - x^2 \rangle} \cong K\left[x, x^2\right] & \longrightarrow & K[x] \\ \sum_{i,j} a_{ij} x^i x^{2j} = \sum_{i,j} a_{ij} x^{2j+i} & \longmapsto & \sum_n b_n x^n \end{array}.$$

Example 1.30. Let $xy - 1 \in K[x, y]$. Then
$$A(X) = \frac{K[x,y]}{\langle xy - 1 \rangle} \cong K\left[x, \frac{1}{x}\right].$$

$A(X)$ cannot be $K[x]$.

Definition 1.31. A **Noetherian** topological space X is a topological space such that if
$$C_1 \supseteq C_2 \supseteq \dots$$
is a decreasing chain of closed sets then there is a k such that $C_k = C_{k+1} = \dots$.

Example 1.32. $\mathbb{A}^n$. Recall that if $A \subset B$ then $I(B) \subset I(A)$. So using the definition above,
$$I(C_1) \subseteq I(C_2) \subseteq \dots.$$
Since $K[x_1, \dots, x_n]$ is Noetherian then $I(C_i)$ stabilises. So $I(C_k) = I(C_{k+1}) = \dots$, but taking Z, we recover C_k so C_k stabilises as well.

Theorem 1.33. *If X is Noetherian then any non-empty closed subset can be expressed as a finite union of irreducible closed sets $X = Y_1 \cup \dots \cup Y_n$. Moreover, if we require that $Y_i \subseteq Y_j$ then this expression is unique.*

Proof. Let C be the collection of closed sets that do not satisfy that property. Let Y be a minimum closed inside C, in particular Y is reducible, so $Y = Y' \cup Y''$, for Y', Y'' closed. Hence $Y', Y'' \not\subset C$, so they can be expressed as a finite union of irreducibles, a contradiction. If $Y_i \not\subset Y_j$, then suppose

$$Y_1 \cup \dots \cup Y_n = X_1 \cup \dots \cup X_n.$$

Then $Y_1 \subset X_1 \cup X_n$, in particular $Y_1 = \bigcup_j (Y_1 \cap X_j)$, so there is a j such that $Y_1 \cap X_j = Y_1$, so $Y_1 \subset X_j$. We can assume $j = 1$ and repeat the same argument to find that $Y_1 = X_1$, so consider $\overline{Y \setminus Y_1} = Y_2 \cup \dots \cup Y_n$. But

$$Y_2 \cup \dots \cup Y_n = X_2 \cup \dots \cup X_n,$$

and the result follows by induction. □

Corollary 1.34. *Any affine variety in $\mathbb{A}^n$ can be expressed equally as a union of irreducible algebraic varieties.*

Definition 1.35. The **dimension** of a topological space is the supremum of n where

$$Y_0 \subset \dots \subset Y_n$$

is a sequence of irreducible closed sets.

Example 1.36. Dimension of $\mathbb{A}^1$ is one.

Definition 1.37. Let A be a ring and $\mathfrak{p}$ be a prime ideal, then the **height** of $\mathfrak{p}$ is the supremum of n where

$$\mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_n \subset \mathfrak{p},$$

where $\mathfrak{p}_i$ are prime. The **Krull dimension** of A is

$$\sup_{\mathfrak{p} \text{ prime}} \textit{height}(\mathfrak{p}).$$

Proposition 1.38. *If Y is affine then* $\dim(Y) = \dim(A(Y))$.

Proof. Let C be a closed and irreducible set $C \subset Y$, then $I(C) \supset I(Y)$, then $I(C)$ is prime. □

Proposition 1.39. *Let K be a field and B be an integral domain which is a finitely generated algebra, then*

- $\dim(B)$ *is the transcendence degree of $K(B)$ over K, and*
- *if $\mathfrak{p} \subseteq B$ is prime, then*

$$\textit{height}(\mathfrak{p}) + \dim\left(\frac{B}{\mathfrak{p}}\right) = \dim(B).$$

Proof. Atiyah Macdonald chapter 11. □

Proposition 1.40 (Krull Hauptidealsatz)**.** *Let A be a Noetherian ring and $f \in A$ not a zero divisor and not a unit. Then every prime ideal containing f has height one.*

Proof. Atiyah Macdonald page 122. □

Lecture 4 Friday 18/01/19

Proposition 1.41. *A Noetherian integral domain A is a UFD if and only if every prime ideal I of height one is principal.*

Theorem 1.42. *An irreducible variety $Y \subseteq \mathbb{A}^n$ has dimension $n-1$ if and only if $Y = Z(f)$ where f is an irreducible polynomial in $K[x_1, \dots, x_n]$.*

Proof.

$\Longrightarrow$ If Y has dimension $n-1$ then $I(Y)$ has height one, by the above proposition $I(Y) = \langle f \rangle$, so $Y = Z(f)$.

$\Longleftarrow$ Let $I = I(Y)$ then I is prime, by the Krull Hauptidealsatz we have that I has height one, so $\dim(Y) = n - 1$.

□

2 Projective varieties

Definition 2.1. The **projective space** $\mathbb{P}^n$ is defined as

$$\mathbb{P}^n = \frac{\mathbb{A}^{n+1} \setminus \{0\}}{\{x \sim \lambda x \mid \lambda \in K^*\}}.$$

A point in $\mathbb{P}^n$ is written as $[a_0 : \dots : a_n] = \overline{(a_0, \dots, a_n)}$.

Definition 2.2. A **graded ring** R is a ring together with a decomposition

$$R = \bigoplus_{d>0} R_d,$$

where R_d are abelian groups and $R_k \cdot R_t \subseteq R_{k+t}$.

Example 2.3. $K[x_0, \dots, x_n]$ is a graded ring, where R_d are monomials of degree d.

Notation 2.4. Let A be $K[x_0, \dots, x_n]$ without the grading and S be $K[x_0, \dots, x_n]$ as a graded ring.

Definition 2.5. An ideal $I \subseteq S$ is **homogeneous** if

$$I = \bigoplus_{d \geq 0} (I \cap S_d).$$

If $f = f_0 + \dots + f_d$, then $f_i \in I$.

Remark 2.6. I is homogeneous if and only if $I = \langle f_0, \dots, f_n \rangle$, where f_i are homogeneous.

Lemma 2.7. *If I, J are homogeneous then*

1. *$I + J$ is homogeneous,*
2. *IJ is homogeneous,*
3. *$I \cap J$ is homogeneous, and*
4. *$\sqrt{I}$ is homogeneous.*

Proof.

4. Let $f = f_0 + \dots + f_d \in \sqrt{I}$ then

$$f^n = (f_0 + \dots + f_d)^n = f_d^n + \dots \in I \qquad \implies \qquad f_d^n \in I \qquad \implies \qquad f_d \in \sqrt{I},$$

so $f - f_d \in \sqrt{I}$, by induction $f_i \in \sqrt{I}$.

□

Definition 2.8. If f is homogeneous of degree k then

$$f(\lambda \cdot x) = \lambda^k \cdot f(x),$$

in particular $f(x) = 0$ if and only if $f(\lambda \cdot x) = 0$, so it makes sense to define

$$Z(f) = \{x \in \mathbb{P}^n \mid f(x) = 0\}.$$

More generally, if $I \subseteq S$ is a homogeneous ideal then

$$Z(I) = \{x \in \mathbb{P}^n \mid f \in I \text{ homogeneous}, \ f(x) = 0\}.$$

Definition 2.9. A subset $X \subseteq \mathbb{P}^n$ is called a **projective variety** if $X = Z(T)$ for some homogeneous ideal T.

Proposition 2.10.

- $Z(S) \cup Z(T) = Z(ST)$.
- $\bigcap_\alpha Z(S_\alpha) = Z(\bigcup_\alpha S_\alpha)$.
- $Z(0) = \mathbb{P}^n$ *and* $Z(1) = \emptyset$.

Definition 2.11. We define the **Zariski topology** on $\mathbb{P}^n$ by taking closed sets to be $Z(T)$ for some T.

Definition 2.12.

- A projective variety is **irreducible** if it is an irreducible topological space.
- An open subset of a projective variety is called a **quasi-projective variety**.
- The **dimension** of a projective variety is its dimension as a topological space.
- If $T \subseteq S$ then
$$I(T) = \langle f \in S \mid f \text{ homogeneous}, \ \forall p \in T, \ f(p) = 0 \rangle .$$

Definition 2.13. If X is a projective variety the **homogeneous coordinate ring** is

$$S(X) = \frac{S}{I(X)}.$$

Definition 2.14. If $f \in S$ is linear and homogeneous, we call $Z(f)$ a **hyperplane**.

Lecture 5
Monday
21/01/19

Proposition 2.15.
$$\begin{array}{cccc} \phi_i & : & U_i = \mathbb{P}^n \setminus Z(x_i) & \longrightarrow & \mathbb{A}^n \\ & & [x_0 : \dots : x_n] & \longmapsto & \left(\dfrac{x_0}{x_i}, \dots, \dfrac{x_n}{x_i} \right) \end{array}$$

is a homeomorphism in the Zariski topology.

Proof. Let $\phi = \phi_0$ and $U = U_0$, let $C \subseteq \mathbb{A}^n$ be a closed set then we claim that $\phi^{-1}(C)$ is closed. Indeed, let $C = Z(S)$, then $\phi^{-1}(C) = Z(S') \cup U$ where

$$S' = \left\{ x_0^d \cdot f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0} \right) \;\middle|\; f \in S \right\}.$$

Similarly, let $A \subseteq U$ is closed, we claim that $\phi(A)$ is closed. Let $\overline{A}$ be its closure in $\mathbb{P}^n$, then $\overline{A} = Z(B)$, so $\phi(A) = Z(B')$ where
$$B' = \{ f(1, x_1, \dots, x_n) \mid f \in B \} .$$

So we conclude that ϕ is a homeomorphism. ☐

Note. $\langle 1 \rangle = S$ and $\langle x_0, \dots, x_n \rangle \subsetneq S$ map to $\emptyset$ under Z. So in order to have a one-to-one correspondence we need the following.

- $Z(I) = \emptyset$ if and only if $\sqrt{I} \supseteq \langle x_0, \dots, x_n \rangle$. If we consider $Z(I)$ in $\mathbb{A}^{n+1}$, note that $x \in Z(I)$ if and only if $\lambda x \in Z(I)$. So $Z(I) = \emptyset$ if and only if $Z(I) \subseteq \{0\}$. So $\sqrt{I} \supseteq \langle x_0, \dots, x_n \rangle$.
- $I(Z(J)) = \sqrt{J}$ if $Z(J) \neq \emptyset$, since $I(Z(J)) = I(Z_a(J)) = \sqrt{J}$.

Corollary 2.16.

$$\left\{ \text{ projective varieties } \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ homogeneous radical ideals not } \langle x_0, \dots, x_n \rangle \right\},$$

$$\left\{ \text{ irreducible projective varieties } \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ homogeneous radical prime ideals } \right\}.$$

Example 2.17. $\mathbb{P}^n$ is irreducible.

Proposition 2.18.

- *$\mathbb{P}^n$ is Noetherian, that is satisfies the descending chain condition.*
- *Every projective variety can be written as a unique union of irreducible projective varieties. We call* ***irreducible components*** *the irreducible varieties in that decomposition.*

Theorem 2.19. *Let $Y \subseteq \mathbb{P}^n$ be an irreducible projective variety. Then*

$$\dim(S(Y)) = \dim(Y) + 1.$$

Proof. Let

$$\begin{array}{cccc} \phi_i & : & U = \mathbb{P}^n \setminus Z(x_i) & \longrightarrow & \mathbb{A}^n \\ & & [x_0 : \dots : x_n] & \longmapsto & \left(\dfrac{x_0}{x_i}, \dots, \dfrac{x_n}{x_i} \right) \end{array},$$

and $Y_i = \phi_i(Y \cap U_i)$. Let

$$\begin{array}{ccc} K[x_1, \dots, x_n] & \longrightarrow & \left(S(Y)_{x_i}\right)_0 \\ f(x_1, \dots, x_n) & \longmapsto & \dfrac{x_i^{\partial f} f\left(\dfrac{x_1}{x_i}, \dots, \dfrac{x_n}{x_i}\right)}{x_i^{\partial f}} \end{array},$$

then

$$A(Y_i) = \frac{K[x_1, \dots, x_n]}{I(Y_i)} \cong \left(S(Y)_{x_i}\right)_0,$$

moreover $S(Y)_{x_i} \cong A(Y_i)\left[x_i, x_i^{-1}\right]$. So

$$\dim(S(Y)) = \dim\left(S(Y)_{x_i}\right) = \dim\left(A(Y_i)\left[x_i, x_i^{-1}\right]\right) = tra\left(K(Y_i)(x_i)\right) = \dim(Y_i) + 1.$$

Therefore if $Y_i \neq \emptyset$, $\dim(Y_i) = \dim(S(Y)) - 1$ for all i, but since U_i cover Y we have $\dim(Y) = \max\{\dim(Y_i)\}$. (Exercise: if $\{U_n\}_n$ is a finite cover of a topological space Y then $\dim(Y) = \max\{\dim(Y_i)\}$) Since $\dim(Y_i)$ are the same if $Y_i \neq \emptyset$, we conclude that $\dim(Y) = \dim(Y_d)$ for some d. ◻

Lecture 6 Tuesday 22/01/19

Proposition 2.20. *Every Noetherian topological space is compact.*

Proof. Let X be a Noetherian topological space and let $\{U_n\}$ be a cover of X. So consider C, the collection of the union of finitely many open sets of $\{U_n\}$. Since X is Noetherian C has a maximum element, say $U_1 \cup \dots \cup U_n$. If $U_1 \cup \dots \cup U_n \subsetneq X$ then there is $x \in X$ not in the union, and we can find another $U_{\alpha_0} \ni x$. But then

$$U_1 \cup \dots \cup U_n \cup U_{\alpha_0} \supsetneq U_1 \cup \dots \cup U_n,$$

a contradiction. So $X = U_1 \cup \dots \cup U_n$. ◻

Corollary 2.21. *$\mathbb{P}^n$, $\mathbb{A}^n$, affine varieties, and projective varieties are all compact in the Zariski topology.*

Definition 2.22. A variety X is **complete** if for any other variety Y, the projection $X \times Y \to Y$ is closed.

Example 2.23. $\mathbb{P}^n$ is complete. $\mathbb{A}^n$ is not complete.

3 Morphisms

Definition 3.1. Suppose Y is a quasi-affine variety and $p \in Y$. We say that a function $f : Y \to \mathbb{A}^1$ is **regular** at p if there are $g, h \in K[x_1, \ldots, x_n]$ and $U \ni p$ such that $f = g/h$ in U with $h \neq 0$. A function is **regular** if it is regular for every $p \in Y$.

Example 3.2. Local is not global. Let $X = Z(x_1x_4 - x_2x_3) \subseteq \mathbb{A}^4$ and $U = X \setminus Z(x_2, x_4)$. Then

$$\begin{array}{cccc} \phi & : & U & \longrightarrow & \mathbb{A}^1 \\ & & (x_1, x_2, x_3, x_4) & \longmapsto & \begin{cases} \dfrac{x_1}{x_2} & x_2 \neq 0 \\ \dfrac{x_3}{x_4} & x_4 \neq 0 \end{cases} \end{array}$$

is a regular function.

Definition 3.3. Let Y be a quasi-projective variety, $f : Y \to \mathbb{A}^1$, and $p \in Y$. We say that f is **regular** at p if there are g, h homogeneous polynomials of the same degree and an open set $U \ni p$ such that $f = g/h$ on U and $h \neq 0$.

Lemma 3.4. *A regular function is continuous.*

Proof. It is enough to show that $f^{-1}(p)$ is closed. Since f is regular $f = g/h$ on some neighbourhood U, then

$$f^{-1}(p) \cap U = Z(g - ph) \cap U.$$

$\square$

Remark 3.5. If X is irreducible then $f = g$ on $U \subseteq X$, then $f = g$ on X. Because the set where $f - g = 0$ is closed and dense.

Definition 3.6. We will use the term **variety** to denote an affine, quasi-affine, projective, or quasi-projective variety.

Definition 3.7. A **morphism** is $f : X \to Y$ if f is continuous and for every $U \subseteq Y$ and every function $g : U \to \mathbb{A}^1$ the composition $g \circ f$ is regular.

Remark 3.8.

- Let $f : X \to Y$ and $g : Y \to Z$ then the composition $g \circ f$ of these two morphisms is the composition of f and g as functions.
- A morphism $f : X \to Y$ is an **isomorphism** if there is a morphism $g : Y \to X$ such that $f \circ g = id$ and $g \circ f = id$.

Definition 3.9. Let X be a variety. Denote the set of all regular functions of X by $\mathcal{O}(X)$. If $p \in X$ the **local ring** at $p \in X$ is

$$\mathcal{O}_p = \varinjlim_{U \ni p} (\mathcal{O}(U)).$$

An element of $\mathcal{O}_p$ is a pair (U, f), where $p \in U$ and f is regular at p, moreover $(U, f) \sim (V, g)$ if $f = g$ on $U \cap V$.

Lecture 7 Friday 25/01/19

Definition 3.10. Let Y be an irreducible variety, the **function field** $K(Y)$ of Y is the field whose elements are pairs (U, f) where U is open and f is regular on U, and

$$(U, f) + (V, g) = (U \cap V, f + g).$$

Remark 3.11.

- $K(Y)$ is indeed a field for if $(U, f) \neq 0$ then $U^{-1} = U \setminus Z(f)$, so $\left(U^{-1}, 1/f\right)$ is the inverse to (U, f).
- $K(Y)$ is the quotient field of $A(Y)$ or $S(Y)$.
- $\mathcal{O}(Y) \hookrightarrow \mathcal{O}_p \hookrightarrow K(Y)$ for all $p \in Y$.

Theorem 3.12. *If $Y \subseteq \mathbb{A}^n$ is an irreducible affine variety with coordinate ring $A(Y)$ then*

1. $\mathcal{O}(Y) = A(Y)$,
2. *for all $p \in Y$, if $\mathfrak{m}_p = \{f \in A(Y) \mid f(p) = 0\}$ then we have a one-to-one correspondence*
$$\{\text{ points of } Y\ \} \qquad \leftrightsquigarrow \qquad \{\text{ maximal ideals of } A(Y)\ \},$$
3. *for all $p \in Y$, $\mathcal{O}_p \cong A(Y)_{\mathfrak{m}_p}$ and $\dim(\mathcal{O}_p) = \dim(Y)$, and*
4. *$K(Y)$ is the quotient field of $A(Y)$.*

Proof.

1. Notice that there is a natural map $A \to \mathcal{O}(Y)$ with kernel $I(Y)$, so there is an injection $A(Y) \hookrightarrow \mathcal{O}(Y)$, that is
$$A(Y) \subseteq \mathcal{O}(Y) \subseteq \bigcap_{p \in Y} \mathcal{O}_p = \bigcap_{\mathfrak{m}_p} A(Y)_{\mathfrak{m}_p} = A(Y),$$
so $A(Y) = \mathcal{O}(Y)$.
2. We know that points of Y correspond to maximal ideals $\mathfrak{m}_p \supseteq I(Y)$. Taking the quotient, we get maximal ideals inside $A(Y)$.
3. There is a natural map $A(Y)_{\mathfrak{m}_p} \to \mathcal{O}_p$, which is injective by $\alpha : A(Y) \hookrightarrow \mathcal{O}(Y)$, and it is surjective by definition of $\mathcal{O}_p$. Moreover,
$$\dim(\mathcal{O}_p) = \dim(A_p)_{\mathfrak{m}_p} = \mathit{height}(\mathfrak{m}_p) = \dim(Y).$$
4. The quotient field of $A(Y)$ is the quotient field of $\mathcal{O}_p$ for all p, by 3, which is $K(Y)$ by definition.

$\square$

Theorem 3.13. *Let $Y \subseteq \mathbb{P}^n$ be irreducible and projective. Then*

1. $\mathcal{O}(Y) = K$,
2. *for all $p \in Y$, $\mathfrak{m}_p$ as before, $\mathcal{O}_p \cong \left(S(Y)_{\mathfrak{m}_p}\right)_0$, and*
3. $K(Y) \cong \left(S(Y)_{(0)}\right)_0$.

Proof. Recall that

$$\begin{array}{cccc} \phi_i & : & U_i = \mathbb{P}^n \setminus Z(x_i) & \longrightarrow & \mathbb{A}^n \\ & & [x_0 : \dots : x_n] & \longmapsto & \left(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}\right) \end{array}$$

gives $\phi_i^* : A(Y_i) \cong \left(S(Y)_{x_i}\right)_0$ and $Y_i = \phi_i(Y \cap U_i)$.

1. $K \subseteq \mathcal{O}(Y)$. Take $f \in \mathcal{O}(Y)$, so f is regular at each Y_i, but $\mathcal{O}(Y_i) \cong A(Y_i)$, also by ϕ_i^*, $A(Y_i) \cong \left(S(Y)_{x_i}\right)_0$. Thus $f = g_i / x_i^{n_i}$, where $n_i = \deg(g_i)$, in particular $x_i^{n_i} f \in S(Y)_{n_i}$. Now, set $N \geq \sum_i n_i$, then $S(Y)_N \cdot f \subseteq S(Y)_N$, so we can iterate this process to obtain $S(Y)_N \cdot f^q \subseteq S(Y)_N$. In particular $x_0^N f \subset S$, hence $S(Y)[f]$ is contained in $x_0^{-N} S(Y)$. Therefore f is integral since $S(Y)[f]$ is finitely generated. There are $a_i \in S$ such that
$$f^k + a_1 f^{k-1} + \dots + a_k = 0.$$
Since f is homogeneous of degree zero we can take the constant terms of a_i and still have an equation, hence $a_i \in K$.
2. Let $p \in Y$, then $p \in Y_i$, by the previous theorem we know that $\mathcal{O}_p \cong A(Y_i)_{\mathfrak{m}_p}$. By ϕ_i^*, $\mathcal{O}_p \cong \left(\left(S(Y)_{x_i}\right)_{\mathfrak{m}_p}\right)_0$, but since $x_i \notin \mathfrak{m}_p$, hence $\mathcal{O}_p \cong \left(S(Y)_{\mathfrak{m}_p}\right)_0$.
3. Recall that the quotient field of Y is $K(Y) = K(Y_i)$, but $K(Y_i)$ is the quotient field of the coordinate ring $A(Y_i)$, by ϕ_i^*, this is $\left(S(Y)_{(0)}\right)_0$.

$\square$

Lecture 8 Monday 28/01/19

Proposition 3.14. *Let X be an irreducible variety and Y be an irreducible affine variety, then we have a bijection*
$$\alpha : Hom(X, Y) \xrightarrow{\sim} Hom(A(Y), \mathcal{O}(X)),$$
the set of morphisms from X to Y to the set of K-algebra homomorphisms.

Proof. Given a morphism $\phi : X \to Y$, by definition of morphism, ϕ takes regular functions at Y to regular functions at X. So if $f \in A(Y)$ then $\phi \circ f \in \mathcal{O}(X)$. Conversely, let $h : A(Y) \to \mathcal{O}(X)$ be a homomorphism of K-algebras. Recall that
$$A(Y) = \frac{A}{I(Y)} = \frac{k[x_1, \dots, x_n]}{I(Y)}.$$
Take $\overline{x_i} \in A(Y)$ and let $y_i = h(\overline{x_i}) \in \mathcal{O}(X)$ and define
$$\begin{array}{cccc} \psi & : & X & \longrightarrow & \mathbb{A}^n \\ & & p & \longmapsto & (y_1(p), \dots, y_n(p)) \end{array}.$$
We claim that $Im(\psi) \subseteq Y$, but since $Y = Z(I(Y))$, it is enough to show that if $f \in I(Y)$ then $f(\psi(p)) = 0$.
$$f(\psi(p)) = f(y_1(p), \dots, y_n(p)) = f(h(\overline{x_1}(p)), \dots, h(\overline{x_n}(p))) = h(f(x_1, \dots, x_n))(p) = 0.$$
$\square$

Lemma 3.15. *If X, Y are as before then $\psi : X \to Y$ is a morphism if and only if $\psi_i = x_i \circ \psi$ are regular functions.*

Proof. Suppose ψ_i are regular functions, then if p is a polynomial $p \circ \psi$ is regular, but since regular functions are quotients of polynomials, we conclude that $f \circ \psi$ is regular for any regular function f. $\square$

Corollary 3.16. *If X, Y are affine then $X \cong Y$ if and only if $A(X) \cong A(Y)$.*

Corollary 3.17. *The correspondence $X \mapsto A(X)$ induces an arrow reversing correspondence between the category of affine varieties and the category of K-integral domains.*

Lecture 9 Tuesday 29/01/19

Lecture 9 is a problem class.
Lecture 10 is a problem class.

Lecture 10 Friday 01/02/19

4 Rational maps

Lecture 11 Monday 04/02/19

Definition 4.1. Let X, Y be varieties. A **rational map** $f : X \dashrightarrow Y$ is a pair (U, f_U) where $U \subseteq X$ is open and f_U is a morphism on U and we identify $(U, f_U) \sim (V, g_V)$ if $f_U = g_V$ on $U \cap V$.

Lemma 4.2. *If X, Y are varieties and $\phi, \psi : X \to Y$ such that $\phi = \psi$ on $U \subseteq X$, then $\phi = \psi$ on X.*

Proof. We can assume that $Y \subseteq \mathbb{P}^n$ for some n, and hence we reduce to the case where $Y = \mathbb{P}^n$. So the product is $\phi \times \psi : X \to \mathbb{P}^n \times \mathbb{P}^n$. Let $\Delta \subseteq \mathbb{P}^n \times \mathbb{P}^n = Z(x_i y_j - x_j y_i)$. Since $\phi = \psi$ on U, $(\phi \times \psi)(U) \subseteq A$, so $(\phi \times \psi)\left(\overline{U}\right) = (\phi \times \psi)(X) \subseteq \Delta$. $\square$

Definition 4.3.

- A **dominant rational map** is a rational map $f : X \dashrightarrow Y$, such that $f_U(U)$ is dense for some, and hence all, (U, f_U).
- A **birational map** is a dominant rational map $f : X \dashrightarrow Y$ such that f admits an inverse $g : Y \dashrightarrow X$.

Theorem 4.4. *For any two varieties X, Y we have a correspondence*

$$\left\{ \text{ dominant rational maps } f : X \to Y \ \right\} \qquad \leftrightsquigarrow \qquad \left\{ \ K\text{-algebra homomorphisms } K(Y) \to K(X) \ \right\}.$$

Proof. Given a rational map $f : X \dashrightarrow Y$ and let $g \in K(Y)$. Let f_U be a representative of f then we have that if $(V, g) = g$, $g \circ f_U \in K(X)$. Since we can cover Y using affine varieties, we can assume Y is affine then $K(Y) = K(A(Y))$. If we start with a homomorphism $\theta : K(Y) \to K(X)$, let $y_1, \dots, y_n \in A(Y)$ be the generators of $A(Y)$, then $\theta(y_i) \in K(X)$. We can find U such that $\theta(y_i)$ are regular at U. Then this induces a map $A(Y) \to \mathcal{O}(U)$. But then we have a morphism $U \to Y$, and moreover this is the inverse of the map we defined previously. $\square$

Definition 4.5.

- A field extension L/K is **separably generated** if there is a transcendence basis $\{x_i\}$ for L/K such that L is a separable algebraic extension of $K(\{x_i\})$.
- Primitive element theorem. If L/K is finite and separable then $L/K(\alpha)$ for some $\alpha \in L$. If L is infinite and $\beta_1, \dots, \beta_n$ are generators for L/K then $\alpha = c_1\beta_1 + \dots + c_n\beta_n$ for $c_i \in K$.
- If K is perfect, any finitely generated extension L/K is separably generated.

Theorem 4.6. *Any variety X of dimension n is birational to a hypersurface $Y \subseteq \mathbb{P}^{n+1}$.*

Proof. Since $K(X) = K$ is finitely generated, by the theorem above it is separably generated. So we can find a transcendence basis $x_1, \dots, x_n \in K$ such that $K/k(x_1, \dots, x_n)$ is finite and separable. By the primitive element theorem, $K = k(x_1, \dots, x_n, y)$ for some y which is algebraic over $k(x_1, \dots, x_n)$, so y is the solution of a polynomial equation f in $k(x_1, \dots, x_n)$. In particular if we clear denominators we get a polynomial $f(x_1, \dots, x_n, y)$ in $\mathbb{A}^{n+1}$, by taking $Z(f)$ we get a hypersurface and taking its projective closure we get a hypersurface in $\mathbb{P}^n$. $\square$

Lecture 12 Tuesday 05/02/19

Corollary 4.7. *The following are equivalent.*

- *$F : X \dashrightarrow Y$ is birational.*
- *There exist U, V such that $F : U \to V$ is an isomorphism.*
- $K(Y) \cong K(X)$.

Definition 4.8. The **blow-up** of $\mathbb{A}^n$ at the origin 0, denoted by $\widetilde{\mathbb{A}^n}$, is

$$Z\left(x_i y_j - x_j y_i\right) \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1}.$$

$$\begin{tikzcd} \widetilde{\mathbb{A}^n} \arrow[r, hook] \arrow[dr, "\pi"'] & \mathbb{A}^n \times \mathbb{P}^{n-1} \arrow[d, "(x,y)\mapsto x"] \\ & \mathbb{A}^n \end{tikzcd}.$$

Proposition 4.9.

1. *Let $P \in \mathbb{A}^n$, if $P \neq 0$ then $\pi^{-1}(P)$ is a single point, and $\widetilde{\mathbb{A}^n} \setminus \pi^{-1}(0) \cong \mathbb{A}^n \setminus \{0\}$.*
2. *$\pi^{-1}(0) \cong \mathbb{P}^{n-1}$.*
3. *Points of $\pi^{-1}(0)$ are in one-to-one correspondence with the set of lines through the origin.*
4. *$\widetilde{\mathbb{A}^n}$ is irreducible.*

Proof.

1. If $P \neq 0$ then $y_j = x_j y_i / x_i$ and this is true for every j, so this gives a unique point in $\mathbb{P}^{n-1}$.
2. Obvious.
3. A line through the origin is given by $x_i = t a_i$ for $t \neq 0$. Taking π^{-1} of this line we get $x_i = t a_i$ and $y_i = t a_i = a_i$. In other words if $x \neq 0$, $\pi^{-1}(X) = (X, [X])$.
4. $\widetilde{\mathbb{A}^n} \setminus \pi^{-1}(0) \cong \mathbb{A}^n \setminus \{0\}$ is dense and irreducible, by 3.

∎

Definition 4.10. If $Y \ni 0$ is a closed subvariety of $\mathbb{A}^n$ we define the **blow-up** of Y at 0 by

$$\widetilde{Y} = \overline{\pi^{-1}(Y \setminus \{0\})}.$$

More generally, we can blow-up any point by taking an affine change of coordinates. We also get a birational map $\pi : \widetilde{Y} \to Y$.

Example 4.11. Let $Y = Z\left(y^2 - x^2(x+1)\right)$. The equations of the blow-up are

$$\begin{cases} y^2 = x^2(x+1) \\ xu = yt \end{cases},$$

where $[t : u] \in \mathbb{P}^1$. Suppose $t \neq 0$.

$$\begin{cases} y^2 = x^2(x+1) \\ y = xu \end{cases} \implies (xu)^2 = x^2(x+1) \implies x^2\left(u^2 - x - 1\right) = 0.$$

Example 4.12. Let $y^2 = x^3$.

$$\begin{cases} y^2 = x^3 \\ y = xu \end{cases} \implies (xu)^2 = x^3 \implies x^2\left(u^2 - x\right) = 0.$$

5 Nonsingular varieties

Lecture 13 Friday 08/02/19

Definition 5.1. Let $Y \subseteq \mathbb{A}^n$ be an affine variety of dimension r, and suppose $I(Y) = \langle f_1, \dots, f_k \rangle$. Y is **nonsingular** at $P \in Y$ if $rank\left(\frac{\partial f_i(P)}{\partial x_j}\right) = n - r$. Y is **nonsingular** if it is nonsingular at every $P \in Y$.

Example 5.2. Let $x^2 = x^4 + y^4 \subseteq \mathbb{A}^2$, so $f = x^2 - x^4 - y^4$.

$$\frac{\partial f}{\partial x} = 2x - 4x^3 = 0 \qquad \implies \qquad x\left(1 - 2x^2\right) = 0 \qquad \implies \qquad x = 0 \text{ or } 2x^2 = 1,$$

$$\frac{\partial f}{\partial y} = -9y^3 = 0 \qquad \implies \qquad y = 0 \qquad \implies \qquad x^2 = x^4 \qquad \implies \qquad x = 0 \text{ or } x^2 = 1,$$

so $Sing(Y) = \{(0,0)\}$.

Example 5.3. Let $Y = Z(f) = Z\left(y^2 - x^3\right)$.

$$\frac{\partial f}{\partial x} = -3x^2 = 0, \qquad \frac{\partial f}{\partial y} = 2y = 0,$$

so $Sing(Y) = \{(0,0)\}$.

Definition 5.4. Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and residue field $A/\mathfrak{m} = K$. A is a **regular local ring** if $\dim_K\left(\mathfrak{m}/\mathfrak{m}^2\right) = \dim(A)$.

Note. $\left(\mathfrak{m}/\mathfrak{m}^2\right)^*$ is called the **Zariski-tangent space**.
Claim that $\mathfrak{m}/\mathfrak{m}^2$ is a K-vector space for $K = A/\mathfrak{m}$.

Theorem 5.5. *Let $Y \subseteq \mathbb{A}^n$ be an affine variety. Then Y is nonsingular at P if and only if $\mathcal{O}_P$ is a regular local ring.*

Proof. Let $P = (a_1, \dots, a_n) \in Y$ with corresponding maximal ideal $I_P = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. We define a map

$$\begin{array}{cccc} \theta_P & : & A = K[x_1, \dots, x_n] & \longrightarrow & K^n \\ & & f & \longmapsto & \left(\dfrac{\partial f(P)}{\partial x_1}, \dots, \dfrac{\partial f(P)}{\partial x_n}\right) \end{array}.$$

Note that $\theta((x_i - a_i)(x_j - a_j)) = 0$, hence $\theta_P\left(I_P^2\right) = 0$, in particular we have an isomorphism $I_P/I_P^2 \cong K^n$. By the isomorphism, if $\alpha = I(Y) = \langle f_1, \dots, f_t \rangle$ then the rank of $\frac{\partial f_i(P)}{\partial x_j}$ corresponds to the dimension of α under the isomorphism, which is $\overline{\alpha}$ in I_P/I_P^2, $(\alpha + I_P)/I_P^2$. Now $\mathcal{O}_P = (A/\alpha)_{I_P}$. If $\mathfrak{m} = (I_P + \alpha)/\alpha$ then $\mathfrak{m}^2 = \left(I_P^2 + \alpha\right)/\alpha$, so $\mathfrak{m}/\mathfrak{m}^2 = I_P/\left(I_P^2 + \alpha\right)$. So

$$r = \dim\left(\frac{\mathfrak{m}}{\mathfrak{m}^2}\right) = \dim\left(\frac{I_P}{I_P^2 + \alpha}\right) = \dim\left(\frac{I_P}{I_P^2}\right) - \dim\left(\frac{I_P^2 + \alpha}{I_P^2}\right) = n - rank\left(\frac{\partial f_i}{\partial x_j}\right).$$

So $\mathcal{O}_P$ is regular if and only if $rank\left(\frac{\partial f_i}{\partial x_j}\right) = n - r$. ☐

Definition 5.6. Let X be a variety. X is **nonsingular** at P if $\mathcal{O}_P$ is a regular local ring.

Theorem 5.7. *Let Y be a variety. Then $Sing(Y)$ is a proper and closed set. The set of nonsingular points of Y is open and dense.*

Proof. Prove that $Sing(Y)$ is closed, first. We know that the rank of the Jacobian is at most $n-r$, therefore the singular points occurs when the rank is less than $n-r$, which is to say that $Sing(Y)$ is given by the vanishing of the $(n-r) \times (n-r)$ minors of $\frac{\partial f_i}{\partial x_j}$ and $I(Y)$, hence is closed. To prove that it is proper $Sing(Y) \subsetneq Y$. ☐

Lecture 14 Monday 11/02/19

Lecture 14 is a problem class.
Lecture 15 is a problem class.

Lecture 15 Tuesday 12/02/19

6 Intersections in projective space

Lecture 16 Friday 15/02/19

Theorem 6.1. *Let $Y, Z \subseteq \mathbb{A}^n$ be varieties, with $\dim(Y) = r$ and $\dim(Z) = s$ then every irreducible component has dimension at least $r + s - n$.*

Proof. Suppose Z is a hypersurface. Then if $Y \subseteq Z$ the theorem holds, and if $Y \nsubseteq Z$ the theorem is true by homework 1. Let Z be general. Consider the diagonal in $\mathbb{A}^{2n}$ given by the image of the isomorphism $P \mapsto P \times P$, then $Y \cap Z$ corresponds to $(Y \times Z) \cap \Delta$. Recall that

$$\Delta = Z(x_1 - y_1) \cap \cdots \cap Z(x_n - y_n),$$

by the first case n times we have that each irreducible component has dimension

$$(r + s) - n - 2n = r + s - n.$$

□

Theorem 6.2. *Let $Y, Z \subseteq \mathbb{P}^n$ be varieties, where $\dim(Y) = r$ and $\dim(Z) = s$, then each irreducible component of $Y \cap Z$ has dimension at least $r + s - n$. Moreover, if $r + s - n \geq 0$ then $Y \cap Z \neq \emptyset$.*

Proof. Take the affine cone of Y and Z, $C(Y)$ and $C(Z)$, since $0 \in C(Y) \cap C(Z)$ we apply the previous theorem to get

$$(r + 1) + (s + 1) - (n + 1) = r + s - n + 1,$$

so therefore $Y \cap Z \neq \emptyset$. □

Definition 6.3. A **numerical polynomial** is a polynomial $f \in \mathbb{Q}[x]$ such that $f(n) \in \mathbb{Z}$ for $n \gg 0$, for n sufficiently large.

Theorem 6.4.

1. *If $f \in \mathbb{Q}[x]$ is a numerical polynomial then there are $c_0, \dots, c_r \in \mathbb{Z}$ such that*

$$f(x) = c_0 \binom{x}{r} + \cdots + c_r \binom{x}{0}.$$

2. *If for $n \gg 0$, $\Delta f = f(n+1) - f(n) = q$ and q is a numerical polynomial, then there exists p such that for $n \gg 0$, $p(n) = f(n)$.*

Proof.

1. By linear algebra we can find $c_0, \dots, c_r \in \mathbb{Q}$ such that

$$f(x) = c_0 \binom{x}{r} + \cdots + c_r \binom{x}{0},$$

then

$$\Delta f = c_0 \binom{x}{r-1} + \cdots + c_{r-1} \binom{x}{0}.$$

By induction on the degree of f we have that $c_0, \dots, c_{r-1} \in \mathbb{Z}$, but since $f(n) \in \mathbb{Z}$ for $n \gg 0$ then $c_r \in \mathbb{Z}$.

2. If

$$q = c_0 \binom{x}{r} + \cdots + c_r \binom{x}{0},$$

set

$$p = c_0 \binom{x}{r+1} + \cdots + c_r \binom{x}{1}.$$

$\Delta p = q$ gives $\Delta(f - p)(n) = 0$.

□

Definition 6.5.

- Let S be a graded ring. A **graded S-module** is a module M with a decomposition
$$M = \bigoplus_{d \in \mathbb{Z}} M_d,$$
such that $S_k \cdot M_d \subseteq M_{d+k}$.
- Let $l \in \mathbb{Z}$. The **twisted module** $M(l)$ is the graded S-module given by $M(l)_k = M_{l+k}$.
- $Ann(M) = \{x \in S \mid xM = 0\}$.

Theorem 6.6. *Let M be a finitely generated graded S-module. Then there is a filtration*
$$0 = M^0 \subseteq \cdots \subseteq M^r = M,$$
such that $M^i/M^{i-1} \cong (S/\mathfrak{p}_i)(l)$ for some $\mathfrak{p}_i$ prime ideals and $l_i \in \mathbb{Z}$, such that

- *prime $\mathfrak{p} \supseteq Ann(M)$ if and only if $\mathfrak{p} \subseteq \mathfrak{p}_i$, that is $\mathfrak{p}_i$ are minimal primes of M, and*
- *for each minimal prime $\mathfrak{p}$ of M the number of times $\mathfrak{p}$ appears in the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ is $len_{S_\mathfrak{p}}(M_\mathfrak{p})$.*

Lecture 17 Monday 18/02/19

Definition 6.7. Let $\mathfrak{p}$ be a minimal prime of a graded S-module M. Then the **multiplicity** of M at $\mathfrak{p}$ is $len_{S_\mathfrak{p}}(M_\mathfrak{p})$.

Definition 6.8. Let M be a graded $S = K[x_1, \dots, x_n]$-module. The **Hilbert function** of M is $\phi_M(l) = \dim_K(M_l)$.

Theorem 6.9. *Let M be a graded $S = K[x_1, \dots, x_n]$-module. Then for $n \gg 0$, there is a unique polynomial $P_M \in \mathbb{Q}[x]$ such that $\phi_M(n) = P_M(n)$. P_M is called the* ***Hilbert polynomial****. It is a polynomial of degree* $\dim(Z(Ann(M)))$.

Proof. By the previous theorem, M has a filtration
$$0 = M^0 \subseteq \cdots \subseteq M^r = M,$$
such that M^i/M^{i-1} is of the form $(S/\mathfrak{p}_i)(l_i)$. Without loss of generality we can assume $M = S/\mathfrak{p}$, since l_i amounts to a translation $z \mapsto z + l_i$. If $\mathfrak{p} = \langle x_0, \dots, x_n \rangle$ then $S/\mathfrak{p} \cong K$, in particular $\phi_M(l_i) = 0$ if $l_i > 0$, but then take $P_M = 0$. We can assume $\dim(0) = -1$ and $\dim(\emptyset) = -1$. Suppose $\mathfrak{p} \neq \langle x_0, \dots, x_n \rangle$. Then there is $x_i \notin \mathfrak{p}$ and consider the short exact sequence
$$0 \to M \xrightarrow{x_i} M \to \frac{M}{x_i M} = M'' \to 0.$$
Taking Hilbert function we get that
$$\phi_{M''}(l) = \phi_M(l) - \phi_M(l-1) = \Delta\phi_M(l-1).$$
Note that $Ann(M'') = Ann(M) \cup \{x_i\}$, so $Z(Ann(M'')) = Z(\mathfrak{p}) \cap Z(x_i)$. Note that
$$\dim(Ann(M'')) = \dim(Z(\mathfrak{p})) - 1,$$
so we apply induction over $\dim(Ann(M))$. Thus $\phi_{M''}$ agrees with a polynomial $P_{M''}(n)$ for $n \gg 0$ but then $\Delta\phi_M = P_{M''}$ for $n \gg 0$, so ϕ_M agrees with a polynomial of degree
$$\dim(Ann(M'')) + 1 = \dim(Z(\mathfrak{p})).$$
∎

Definition 6.10. If $Y \subseteq \mathbb{P}^n$ of dimension r, the **Hilbert polynomial** of Y is the Hilbert polynomial of $S(Y)$. The degree of Y is $r!$ times the leading coefficient of P_Y.

Theorem 6.11.

1. *If* $Y \neq \emptyset$, *then* $\deg(Y) \in \mathbb{Z}_{>0}$.
2. $\deg(\mathbb{P}^n) = 1$.
3. *If* $Y = Y_1 \cup Y_2$ *with* $\dim(Y_i) = r$ *and* $\dim(Y_1 \cap Y_2) < r$ *then* $\deg(Y) = \deg(Y_1) + \deg(Y_2)$.
4. *If* H *is a hypersurface generated by* f *then* $\deg(H) = \deg(f)$.

Proof.

1. Obvious.
2. $$\phi_{\mathbb{P}^n}(z) = \binom{z+n}{n} = \frac{1}{n!}(z)\dots(n+1) = \frac{1}{n!}z^n + \dots.$$
3. Let $I = I(Y)$, $I_1 = I(Y_1)$, and $I_2 = I(Y_2)$. Consider the short exact sequence
$$0 \to \frac{S}{I} \to \frac{S}{I_1} \oplus \frac{S}{I_2} \to \frac{S}{I_1 + I_2} \to 0.$$
Taking Hilbert function,
$$\phi_{\frac{S}{I_1+I_2}} = \phi_{\frac{S}{I_1} \oplus \frac{S}{I_2}} - \phi_{\frac{S}{I}}.$$
Since $Z(I_1 + I_2) = Y_1 \cap Y_2$ and $\dim(Y_1 \cap Y_2) < r$ we have that $\phi_{S/I_1 \oplus S/I_2}$ and $\phi_{S/I}$ have the same leading coefficients, hence $\deg(Y) = \deg(Y_1) + \deg(Y_2)$.
4. Suppose $\deg(f) = d$ then consider the short exact sequence
$$0 \to S(-d) \xrightarrow{f} S \to \frac{S}{\langle f \rangle} \to 0.$$
Taking Hilbert functions,
$$\phi_{\frac{S}{\langle f \rangle}}(z) = \phi_S(z) - \phi_S(z-d) = \binom{z+n}{n} - \binom{z-d+n}{n} = \frac{d}{(n-1)!}z^{n-1} + \dots.$$

$\square$

Let $Y \subseteq \mathbb{P}^n$ be a projective variety and H a hypersurface then $Y \cap H = Z_1 \cup \dots \cup Z_k$, where each Z_j has dimension $r - 1 = \dim(Y) - 1$. Suppose $I(Z_j) = \mathfrak{p}_j$, then each $\mathfrak{p}_j$ is a minimal prime of $S/(I_Y + I_H)$, then the **intersection multiplicity** $i(Y, H; Z_j)$ is the multiplicity of $S/(I_Y + I_H)$ at $\mathfrak{p}_j$. Lecture 18 Tuesday 19/02/19

Theorem 6.12. *Let $Y \subseteq \mathbb{P}^n$ be a variety and H a hypersurface such that $Y \nsubseteq H$. If $Y \cap H = Z_1 \cup \dots \cup Z_k$ then*

$$\sum_{j=1}^{k} i(Y, H; Z_j) \deg(Z_j) = \deg(Y) \deg(H).$$

Corollary 6.13 (Bézout's theorem)**.** *If $Y, H \subseteq \mathbb{P}^2$ are curves and $Y \cap H = \{P_1, \dots, P_k\}$ then*

$$\sum_{j=1}^{k} i(Y, H; P_j) = \deg(Y) \deg(H).$$

Proof. Supppose H is generated by f, where $\deg(f) = d$, and let $I = I(Y)$.

$$0 \to \left(\frac{S}{I}\right)(-d) \xrightarrow{f} \frac{S}{I} \to \frac{S}{I + I_H} \to 0.$$

Taking Hilbert polynomials we get

$$\phi_{\frac{S}{I_1 + I_2}}(z) = \phi_{\frac{S}{I_Y}}(z) + \phi_{\frac{S}{I_Y}}(z - d).$$

Let $\deg(Y) = e$, then the right hand side is

$$\frac{e}{r!} z^r + \dots - \left(\frac{e}{r!}(z - d)^r + \dots\right) = \frac{de}{(r-1)!} z^{r-1} + \dots.$$

Now on the left hand side, by the structure theorem, there is a filtration

$$0 = M^0 \subseteq \dots \subseteq M^s = M,$$

where $M = S/(I_Y + I_H)$. Then

$$P_M = \sum_{i=1}^{s} P_i = \sum_{i=1}^{s} P_{\frac{M^i}{M^{i-1}}},$$

where each $M^i/M^{i-1} = (S/\mathfrak{p}_i)(l_i)$. Since we want to compare the leading coefficient from this with the one from the right hand side, we only care about the P_i's with degree $r - 1$. So the $\mathfrak{p}_j = I(Z_j)$ and the leading term is

$$\frac{\sum_{j=1}^{k} i(Y, H; Z_j) \deg(Z_j)}{(r-1)!} + \dots.$$

$\square$

7 The 27 lines on a cubic surface

Lecture 19 Friday 22/02/19

Theorem 7.1. *Let $S \subseteq \mathbb{P}^3$ be a nonsingular cubic surface given by a polynomial $f(x, y, z, t)$. Then S has exactly 27 lines.*

We start with a lemma.

Lemma 7.2.

1. *Given a point $p \in S$ then there are at most three lines through p. If there are two or three they must be spheres.*
2. *Every plane π intersect S in*
   - *an irreducible cubic,*
   - *a conic and a line, or*
   - *three distinct lines.*

Proof.

1. $l \subseteq S$ gives $T_p(l) = l \subseteq T_p(S)$, by 2, $T_p(S)$ intersect S in at most three lines.
2. We have to prove that there are no multiple lines in the intersection $S \cap \pi$. Changing coordinates if necessary, we can suppose $\pi = \{f = 0\}$ and $l = \{z = 0\}$ is the line in the intersection.

$$f = z^2 \cdot a(x, y, z, t) + t \cdot b(x, y, z, t).$$

   Claim that S is singular at $z = t = b = 0$.

$$Jac(f) = \begin{pmatrix} z^2 a_x + t b_x & z^2 a_y + t b_y & 2za + z^2 a_z + t b_z & z^2 a_t + b + t b_t \end{pmatrix}.$$

   Since S is smooth there are no multiple lines.

□

Lemma 7.3. *S has a line.*

Proof.

- Let $P \in S$ and consider $T_P(S)$. Then $T_P(S)$ intersects S in a plane cubic $C = S \cap T_P(S)$ which is singular at P. Otherwise we are done. Then C has to be a nodal or a cuspidal curve. So assume that C is a cuspidal curve, and change coordinates if necessary, assume that $P = [0 : 0 : 1 : 0]$ and $T_P(S) = \{t = 0\}$. So the equation of f has the shape

$$f = x^2 z - y^3 + gt,$$

  for some g of homogeneous degree two.

- We consider the point $P_\alpha = \left[1 : \alpha : \alpha^3 : 0\right] \in C \subset S$, consider the plane $x = 0$ and the line $P_\alpha Q$ in $\mathbb{P}^3$ passing through P_α and intersecting this plane $x = 0$ at $Q = (0, y, z, t)$. The line through P_α and Q is $\lambda P_\alpha + \mu Q$ and it lies inside S if

$$f(\lambda P_\alpha + \mu Q) = 0.$$

  After expanding this we have

$$P_\alpha Q \subset S \qquad \iff \qquad A(y, z, t) = B(y, z, t) = C(y, z, t) = 0,$$

  for A, B, C to be determined. There is a polynomial $R(\alpha)$ of degree 27 such that $R(\alpha) = 0$ if and only if $A = B = C$ have a common zero.

Lecture 20 Monday 25/02/19

- Let $f(x,y,z,t)$ be a polynomial, then the **polar form** of f is

$$f_1(x,y,z,t,x',y',z',t') = \frac{\partial f}{\partial x} \cdot x' + \frac{\partial f}{\partial y} \cdot y' + \frac{\partial f}{\partial z} \cdot z' + \frac{\partial f}{\partial t} \cdot t',$$

where $P = (x,y,z,t)$ and $Q = (x',y',z',t')$. Then

$$f(\lambda P + \mu Q) = \lambda^3 f(P) + \lambda^2 \mu f_1(P,Q) + \lambda \mu^2 f_1(Q,P) + \mu^3 f(Q).$$

The polar form of $f = x^2 z - y^3 + gt$ is

$$f_1 = 2xzx' - 3y^2 y' + x^2 z' + g(x,y,z,t)\, t' + t g_1,$$

where g_1 is the polar form of g. Recall $P_\alpha = \left(1, \alpha, \alpha^2, 0\right)$ and $Q = (0,y,z,t)$, so

$$\{f(\lambda P + \mu Q) = 0\} = PQ \subseteq S \qquad \iff \qquad f(P) = f_1(P,Q) = f_1(Q,P) = f(Q) = 0.$$

Thus

$$\begin{cases} A = z - 3\alpha^2 y + g\left(1, \alpha, \alpha^3, 0\right) t \\ B = -3\alpha y^2 + g_1\left(1, \alpha, \alpha^3, 0, 0, y, z, t\right) t \\ C = -y^3 + g(0,y,z,t)\, t \end{cases}.$$

- Note that

$$g\left(1, \alpha, \alpha^3, 0\right) = a^6 + \dots.$$

If $l = 0$,

$$z = 3\alpha^2 y + g(P)\, t = 3\alpha^2 y + \left[a^6\right] t.$$

Applying this to $B = 0$ we have

$$B = -3\alpha y^2 + g_1\left(1, \alpha, \alpha^3, 0, 0, y, 3\alpha^2 y - \left[a^6\right] t, t\right) t = b_0 y^2 + b_1 y t + b_2 t^2,$$

where

$$b_0 = -3\alpha, \qquad b_1 = 6\alpha^5 + \dots, \qquad b_2 = -2\alpha^9 + \dots.$$

Substituting z in C we get

$$C = c_0 y^3 + c_1 y^2 t + c_2 y t^2 + c_3 t^3,$$

where

$$c_0 = -1, \qquad c_1 = 9\alpha^4 + \dots, \qquad c_2 = -6\alpha^8 + \dots, \qquad c_3 = \alpha^{12} + \dots.$$

By Sylvester theorem B and C have a common zero if and only if

$$\det \begin{pmatrix} -3\alpha & 6\alpha^5 & -2\alpha^9 & & \\ & -3\alpha & 6\alpha^5 & -2\alpha^9 & \\ & & -3\alpha & 6\alpha^5 & -2\alpha^9 \\ -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} & \\ & -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} \end{pmatrix} = 0.$$

if and only if

$$\alpha^{27} \det \begin{pmatrix} -3 & 6 & -2 & & \\ & -3 & 6 & -2 & \\ & & -3 & 6 & -2 \\ -1 & 9 & -6 & 1 & \\ & -1 & 9 & -6 & 1 \end{pmatrix} = \alpha^{27} + \dots = 0.$$

This concludes the proof that S has a line because we know that the matrix has at least one root and for each root we get a value of α such that the line $P_\alpha Q \subseteq S$.

$\square$

Lecture 21 Tuesday 26/02/19

Proposition 7.4. *Let l be a line in S, then there are five pairs of lines (l_i, l_i') intersecting l such that*

- *$l \cup l_i \cup l_i'$ is coplanar, and*
- *$(l_i \cup l_i') \cap (l_j \cup l_j') = \emptyset$.*

Proof. Given any plane $\Pi \subseteq \mathbb{P}^3$, if Π contains a line l of S then $\Pi \cap S$ is l and a conic. l is given by $z = t = 0$.

$$f = Ax^2 + Bxy + Cy^2 + Dx + Ey + F, \qquad A, B, C, D, E, F \in K[z, t].$$

We want to prove that there are exactly five planes Π_i such that $f|_{\Pi_i}$ is a singular conic. The conic given by f is singular if and only if

$$\Delta = \det \begin{pmatrix} A & B & D \\ B & C & E \\ D & E & F \end{pmatrix} = 4ACF + BDE - AE^2 - B^2F - CD^2 = 0.$$

Δ is four times the usual determinant if *char* $(K) \neq 2$. Notice that Δ is a form of degree five in two variables z and t. We know that l, l_i, l_i' could be of two types.

1. $l : (t = 0)$, $l_1 : (x = 0)$, $l_1' = (y = 0)$.
2. $l : (t = 0)$, $l_1 : (x = 0)$, $l_1' = (x = t)$.

Assume we are in case 1. Suppose $z = 0$ is a solution, then we have to prove that z^2 is not a solution. Then the equation of f is

$$f = txy + gz.$$

So $B = t + az$, where $a \in K$, then $\Delta \equiv -t^2F \mod z^2$. If $F \neq 0$ then Δ is non-zero, but F is non-zero because F is nonsingular, thus there are no multiple roots. ☐

Corollary 7.5. *S has at least two distinct lines.*

Proof. Just take l_1 and l_2. ☐

Lemma 7.6. *If $l_1, \dots, l_4 \in \mathbb{P}^3$ are disjoint lines then*

- *either all four lines lie on a smooth quadric and they have an infinite number of transversals,*
- *or the four lines do not lie in any quadric and they have either one or two common transversals.*

Proof. Any three lines lie in a smooth quadric Q. ☐

Lemma 7.7.

- *Any line not the 17 lines intersect exactly three of the lines $l_1, \dots, l_5$.*
- *Conversely, given $ijk \subset \{1, 2, 3, 4, 5\}$ there is a line passing through l_i, l_j, l_k.*

8 Grassmannians

Lecture 22
Friday
01/03/19

Definition 8.1. Let V be a vector space of dimension n, then

$$G(k;n) = \{S \subseteq V \mid S \text{ subspace of dimension } k\}.$$

Remark 8.2. A point in $G(k;n)$ can be expressed as a basis $[v_1, \dots, v_k]$ for a k-dimensional space.

Theorem 8.3. *The map*

$$\begin{array}{rrcl} p & : \qquad G(k;n) & \longrightarrow & \mathbb{P}\left(\bigwedge^k (V)\right) \cong \mathbb{P}^{{}^nC_k - 1} \\ & [v_1, \dots, v_k] & \longmapsto & [v_1 \wedge \dots \wedge v_k] \end{array}$$

is an embedding. That is, image of p is closed.

Example 8.4. Claim that a line $L \subseteq \mathbb{P}^3$ gives a point in $G(2;4) \hookrightarrow \mathbb{P}^5$. $G(2;4)$ is a quadric in $\mathbb{P}^5$ given by $Z(xs - yt + zw)$.

Proof. Now we will see the coordinates of the map p. Given a vector space V of dimension n and a vector subspace $S \subseteq V$ of dimension k, then let $v_1, \dots, v_n$ be a basis for V, and $s_1, \dots, s_k$ be a basis for S, then the basis for S can be seen as a $k \times n$ matrix

$$M_S = \begin{pmatrix} s_{11} & \dots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{k1} & \dots & s_{kn} \end{pmatrix}.$$

If we change the basis for S then the matrix above gets multiplied by an invertible $k \times k$ matrix. Then this $k \times k$ matrix acts on the $k \times k$ minors of M_S. Suppose the first minor K_1 is non-zero then choose the inverse of that minor as a base change so that M_S will have the form

$$\begin{pmatrix} 1 & & & b_{11} & \dots & b_{1n-k} \\ & \ddots & & \vdots & \ddots & \vdots \\ & & 1 & b_{k1} & \dots & b_{kn-k} \end{pmatrix}.$$

This gives a correspondence between matrices M_S with first non-zero minor and $\mathbb{A}^{k(n-k)}$. Therefore, the image of p has dimension $k(n-k)$. ☐

Similarly, we can define flag varieties. Given a vector space V and **flag**

$$0 \subseteq V_1 \subseteq \dots \subseteq V_n \subseteq V$$

of vector subspaces of dimension V_i, the **flag variety** denoted by $F(V)$ is the set of flags on V.

9 Divisors on curves

Definition 9.1. A **Weil divisor** is a formal finite sum

$$D = \sum_i a_i Y_i, \qquad a_i \in \mathbb{Z},$$

of algebraic subvarieties of codimension one.

Definition 9.2. More generally, an **algebraic cycle** is a formal sum of codimension p subvarieties

$$C = \sum_i a_i Y_i \subseteq X, \qquad a_i \in \mathbb{Z}.$$

By integrating algebraic cycles, we get a map from the space of p-cycles into the cohomology of the variety. **Hodge conjecture** states that this defines a bijection.

Example 9.3. In case $\dim(X) = 1$, then a divisor is just a sum of points with multiplicity. If $K = \mathbb{C}$ and

$$f = \frac{(z-1)(z-2)}{(z-3)(z-4)},$$

then $(f) = \overline{1} + \overline{2} - \overline{3} - \overline{4}$.

Definition 9.4. Let $K = \mathbb{C}$ and $\dim(X) = 1$. Let $D, V \subseteq X$. Then **linear equivalence** is $D \sim V$ if and only if $D - V = (f)$ for $f \in K(x)$.

Definition 9.5. The **class group** is divisors modulo $\sim$.

Definition 9.6. Let $X \subseteq Y$ be a subvariety, then

$$\mathcal{O}_{X,Y} = \{(U, f) \mid f \text{ regular at } U,\ U \cap Y \neq \emptyset\}.$$

Let f be a rational function, then

$$(f) = \sum_Y v_Y(f) Y,$$

where v_Y is the valuation associated to $\mathcal{O}_{X,Y}$.

Lecture 23
Monday
04/03/19

Definition 9.7. Let X be a smooth projective curve.

- A **divisor** D is a formal sum $K_1 p_1 + \cdots + K_n p_n$ of points, where $K_i \in \mathbb{Z}$,
- We say a divisor D is **effective** if $K_i \geq 0$.
- Given two divisors D, E, $D \geq E$ if and only if $D - E \geq 0$.
- The **degree** of D, denoted $\deg(D)$, is the sum $\sum_{i=1}^n K_i$.

Remark 9.8. Degree gives a map $\deg : Div \to \mathbb{Z}$. The set of all divisors on X has a natural group structure given by addition, we denote this group by $Div(X)$.

Notation 9.9. The subgroup of **degree zero divisors** is denoted by $Div^0(X)$.

Definition 9.10.

- For a non-zero homogeneous polynomial $f \in S(X)$ the **divisor** of f is
$$(f) = div(f) = \sum_{a \in V_X(f)} mult_a(f) \cdot a \in Div(f).$$
By Bézout's theorem, $\deg(div(f)) = \deg(X)\deg(f)$.
- If $Y \subseteq \mathbb{P}^2$ not containing X, then the **intersection** of X and Y is
$$X \cdot Y = \sum_{a \in X \cap Y} mult_a(X, Y) \cdot a.$$

Example 9.11. Let $X = Z(xz - y^2)$ and $Y = Z(z)$ then $X \cap Y = \{[1 : 0 : 0]\}$, so
$$X \cdot Y = 2 \cdot [1 : 0 : 0].$$

Lemma 9.12. *$mult_a(fg) = mult_a(f) + mult_a(g)$ gives $div(fg) = div(f) + div(g)$.*

Proof. Recall that $mult_a(f) = len(\mathcal{O}_a / \langle f \rangle) = \dim_K(\mathcal{O}_a / \langle f \rangle)$. Thus there is a short exact sequence
$$0 \to \frac{\mathcal{O}_a}{\langle f \rangle} \xrightarrow{g} \frac{\mathcal{O}_a}{\langle fg \rangle} \to \frac{\mathcal{O}_a}{\langle g \rangle} \to 0.$$
□

Definition 9.13. Let $f \in K^*(X)$, then if $f = g/h$ we define $mult_a(f) = mult_a(g) - mult_a(h)$.

If we take a different representation of f, say $f = g'/h'$, then $g/h = g'/h'$ gives $gh' = hg'$, so
$$\begin{cases} mult_a(gh') = mult_a(g) + mult_a(h') \\ mult_a(hg') = mult_a(h) + mult_a(g') \end{cases} \implies mult_a(g) - mult_a(h) = mult_a(g') - mult_a(h').$$

Analogously, we have
$$div(f) = \sum_{a \in Z(g) \cup Z(h)} mult_a(f)\, a = div(g) \cdot div(h).$$

Example 9.14. Let $f = xy/(x-y)^2$ on $\mathbb{P}^1$. Then
$$div(f) = [1 : 0] + [0 : 1] - 2[1 : 1].$$

Remark 9.15. Note that $\deg(div(f))$ is always zero because
$$\deg(div(f)) = \deg(div(g)) - \deg(div(h)) = (\deg(X))(\deg(g)) - (\deg(X))(\deg(h)) = 0.$$

Definition 9.16. A divisor on X is called principal if it is of the form $div(f)$ for some $f \in K^*(X)$. We denote the subgroup of all principal divisors by $Prin(X)$.

Definition 9.17. The quotient
$$Pic(X) = \frac{Div(X)}{Prin(X)}$$
is called the **Picard group** of X. Restricting to degree zero divisors, we get
$$Pic^0(X) = \frac{Div^0(X)}{Prin(X)},$$
where $Div^0(X)$ are the divisors of degree zero.

By the degree map $\deg : Div(X) \to \mathbb{Z}$ we have
$$\frac{Pic(X)}{Pic^0(X)} \cong \frac{Div(X)}{Div^0(X)} \cong \mathbb{Z}.$$

Example 9.18. Every degree zero divisor is principal. Suppose

$$D = K_1 [a_{1,0} : a_{1,1}] + \dots + K_n [a_{n,0} : a_{n,1}], \qquad \sum_{i=1}^{n} K_i = 0,$$

then set

$$f [x_0 : x_1] = \prod_{i=1}^{n} (a_{i,1} x_0 - a_{i,0} x_1)^{K_i}.$$

So $Pic^0 (\mathbb{P}^1) = \{0\}$ so $Pic (\mathbb{P}^1) = \mathbb{Z}$.

Lecture 24 Tuesday 05/03/19

Lemma 9.19 (Nakayama lemma)**.** *If R is local with maximal ideal $\mathfrak{m}$ and M is finitely generated then $M = \mathfrak{m} M$ gives $M = 0$.*

Corollary 9.20. *If R is local with maximal ideal $\mathfrak{m}$ then $\langle t_1, \dots, t_n \rangle = \mathfrak{m}$ if and only if $\langle \overline{t_1}, \dots, \overline{t_n} \rangle = \mathfrak{m}/\mathfrak{m}^2$.*

Proof. Let $N = \langle t_1, \dots, t_n \rangle \subseteq \mathfrak{m}$. Suppose $\langle \overline{t_1}, \dots, \overline{t_m} \rangle = \mathfrak{m}/\mathfrak{m}^2$. Then

$$N + \mathfrak{m}^2 = \mathfrak{m} + \mathfrak{m}^2 \qquad \implies \qquad \frac{N + \mathfrak{m}^2}{N} = \frac{\mathfrak{m} + \mathfrak{m}^2}{N} \qquad \implies \qquad \mathfrak{m} \left(\frac{\mathfrak{m}}{N} \right) = \frac{\mathfrak{m}}{N} \qquad \implies \qquad \frac{\mathfrak{m}}{N} = 0,$$

so $\langle t_1, \dots, t_n \rangle = \mathfrak{m}$. $\square$

Lemma 9.21. *Let $X \subseteq \mathbb{P}^2$ be a smooth curve, and $I_a \subseteq \mathcal{O}_a$ be the maximal ideal of the local ring $\mathcal{O}_a$.*

1. *I_a is principal, so $I_a = \langle \phi_a \rangle$ with $mult_a (\phi_a) = 1$.*
2. *Any non-zero $\phi \in \mathcal{O}_a$ can be written as $c \phi_a^m$, where $m = mult_a (\phi)$.*

Proof.

1. Since $\mathcal{O}_a$ is regular, $\dim (\mathfrak{m}/\mathfrak{m}^2) = 1$, in particular $\mathfrak{m} \neq \mathfrak{m}^2$ and we can find $\phi_a \in \mathfrak{m} \setminus \mathfrak{m}^2$, so $\langle \phi_a \rangle = \mathfrak{m}$. Thus any ideal has to be of the form $\langle \phi_a^k \rangle$ since $\langle \phi_a \rangle$ is maximal.
2. Take $\phi \in \mathcal{O}_a$ non-zero then $\langle \phi \rangle = \langle \phi_a^m \rangle$ gives $\phi = c \phi_a^m$, so

$$mult (\phi) = mult (c \phi_a^m) = mult (c) + mult (\phi_a^m) = m \cdot mult (\phi_a) = m.$$

$\square$

Lemma 9.22. *Let $X \subseteq \mathbb{P}^2$ be a smooth curve, and $a \in X$.*

1. *If $f, g \in S$, of same degree with $mult (X, f) \geq m$ and $mult (X, g) \geq m$ then*
   - *$mult_a (X, \lambda f + \mu g) \geq m$, and*
   - *there exist λ, μ such that $mult_a (X, \lambda f + \mu g) \geq m + 1$.*
2. *Let $Y \subseteq \mathbb{P}^2$ be another curve and $m = mult_a (X, Y)$. If $f \in S$ with $mult_a (X, f) \geq m$ then $mult_a (Y, f) \geq m$.*

Proof.

1. Write $f = u \phi_a^m$ and $g = v \phi_a^m$, so for any λ, μ we have $\lambda f + \mu g = (\lambda u + \mu v) \phi_a^m$ so $mult_a (\lambda f + \mu g) \geq m$, and we can find λ', μ' such that $\lambda' u + \mu' v = 0$ at a, so that $mult_a (\lambda f + \mu g) \geq m + 1$.
2. Let $I (X) = \langle g \rangle$, $I (Y) = \langle h \rangle$, and $k = mult_a (X, f) \geq m = mult_a (X, h)$. $f = u \phi_a^k$ and $h = v \phi_a^m$, so $\langle f \rangle \subset \langle h \rangle$. $\langle f, g \rangle \subset \langle g, h \rangle$, and we also have $\langle f, h \rangle \subset \langle g, h \rangle$, so $mult_a (f, h) \geq mult_a (g, h)$ gives $mult_a (Y, f) \geq mult_a (X, Y) = m$.

$\square$

Lemma 9.23. *Let $X \subset \mathbb{P}^2$ be smooth and $g, h \in S(X)$.*

1. *If $div(g) = div(h)$ then g, h are linearly dependent on $S(X)$.*
2. *If h is linear and $div(g) \geq div(h)$ then $h \mid g$ in $S(X)$.*

Proof.

1. By Bézout's theorem, $\deg(X) \cdot \deg(g) = \deg(X) \cdot \deg(h)$, so $\deg(g) = \deg(h)$. We know by the previous lemma that $mult_a(\lambda g + \mu h) \geq m_a$, and we can find $b \in X$ such that $mult_b(\lambda g + \mu h) \geq m_b + 1$. Summing up, we have
$$\sum_{a \in X} mult_a(\lambda g + \mu h) \geq d \deg(X) + 1,$$
but $\lambda g + \mu h$ has degree d, so this is a contradiction unless $\lambda g + \mu h = 0$, that is g, h are linearly dependent.
2. Exercise.

$\square$

Proposition 9.24. *Let $X \subseteq \mathbb{P}^2$ be a smooth cubic. Then for all distinct $a, b \in X$ we have $a - b \neq 0$, so there is no rational function ϕ such that $div(\phi) = a - b$.*

Proof. Assume that the result is false. Then there are $f, g \in S(X)$ of degree d such that

- there are points $a_1, \dots, a_{3d-1}$ and $a \neq b$ on X such that
$$div(g) = a_1 + \dots + a_{3d-1} + a, \qquad div(f) = a_1 + \dots + a_{3d-1} + b,$$
- among $a_1, \dots, a_{3d-1}$, there are at least $2d$ distinct points, since we can multiply f and g by a linear polynomial with distinct roots so the degree increases by one but the number of distinct points increases by three.

Pick a minimal d. If $d = 1$ then
$$div(g) = a_1 + a_2 + a, \qquad div(f) = a_1 + a_2 + b,$$
so $a = b = \Psi(a_1, a_2)$, a contradiction. So $d > 1$. Consider $(\lambda f + \mu g)$, so
$$div(\lambda f + \mu g) \geq a_1 + \dots + a_{3d-1}.$$
We can choose λ, μ such that
$$div(\lambda f + \mu g) \geq a_1 + \dots + a_{3d-1} + c,$$
for any given c. By Bézout's theorem,
$$div(\lambda f + \mu g) = a_1 + \dots + a_{3d-1} + c.$$
So we can choose a and b, so that $a = \Psi(a_1, a_2)$ and $b = \Psi(a_1, a_3)$.
$$div(f) = (a_1 + a_2 + \Psi(a_1, a_2)) + a_3 + \dots + a_{3d-1}, \qquad div(g) = (a_1 + a_3 + \Psi(a_1, a_3)) + a_2 + \dots + a_{3d-1}.$$
Set l, l' linear polynomials such that
$$div(l) = a_1 + a_2 + \Psi(a_1, a_2), \qquad div(l) = a_1 + a_3 + \Psi(a_1, a_3).$$
The quotient by $div(l)$ and $div(l')$ gives a polynomial whose divisor is
$$a_4 + \dots + a_{3d-1} + a_3, \qquad a_4 + \dots + a_{3d-1} + a_2,$$
but since we chose d minimum this gives a contradiction. $\square$

10 Elliptic curves

Definition 10.1. An **abelian variety** A is a smooth connected projective variety which has a group structure such that addition and taking inverse are regular functions. Lecture 25 Friday 08/03/19

Definition 10.2. An **elliptic curve** is a one-dimensional abelian variety.

Proposition 10.3. *Let X be an elliptic curve in $\mathbb{P}^2$, and fix $a_0 \in X$, then there is a bijection*

$$\begin{array}{cccccc} \Phi & : & X & \longrightarrow & Pic^0(X) = \dfrac{Div^0(X)}{Prin(X)} & . \\ & & a & \longmapsto & a - a_0 & \end{array}$$

Proof.

- Φ is injective by the last proposition.
- Φ is surjective. Suppose

  $$D = a_1 + \dots + a_m - b_1 - \dots - b_m.$$

  Consider the function l with $div(l) = a_1 + a_2 + \Psi(a_1, a_2)$, so

  $$D = D + div(l) = div(l) - \Psi(a_1, a_2) + a_3 + \dots.$$

  So we can assume $D = a_1 - b_1 = \Phi(\cdot)$.

  $$a_0 + a_1 + \Psi(a_0, a_1) - b_1 - \Psi(a_0, a_1) - \Psi(b_1, \Psi(a_0, a_1)) = 0,$$

  so

  $$D = a_1 - b_1 = \Psi(b_1, \Psi(a_0, a_1)) - a_0 = \Phi(\Psi(b_1, \Psi(a_0, a_1))).$$

  Thus Φ is surjective.

□

We know that $X \cong Pic^0(X)$, which is a group. But what is the expression for $g_1 + g_2$ for $g_1, g_2 \in X$? $\Phi(g_1 + g_2) = \Phi(g_1) + \Phi(g_2)$, so

$$\begin{aligned} g_1 + g_2 &= \Phi^{-1}(\Phi(g_1) + \Phi(g_2)) = \Phi^{-1}(g_1 - g_0 + g_2 - g_0) = \Phi^{-1}(\Psi(g_0, \Psi(g_1, g_2)) - g_0) \\ &= \Phi^{-1}(\Phi(\Psi(g_0, \Psi(g_1, g_2)))) = \left(\Phi^{-1} \circ \Phi\right)(\Psi(g_0, \Psi(g_1, g_2))) = \Psi(g_0, \Psi(g_1, g_2)). \end{aligned}$$

Let X be an elliptic curve and $a_0 \in X$, can consider the group law based on a_0. Then for $n \in \mathbb{Z}$, we can define $n \times a = a + \dots + a$.

Note. Given $a, b \in X$, the problem of finding whether or not there exists n such that $a = n \times b$ is extremely hard.

Lecture 26 is a problem class. Lecture 26 Monday 11/03/19
Lecture 27 is a problem class. Lecture 27 Tuesday 12/03/19
Lecture 28 is a problem class. Lecture 28 Friday 15/03/19
Lecture 29 is a problem class. Lecture 29 Monday 18/03/19
What's next in Lecture 30? Lecture 30 Tuesday 19/03/19