Algebraic Geometry Notes

Raman Aliakseyeu

Winter 2024

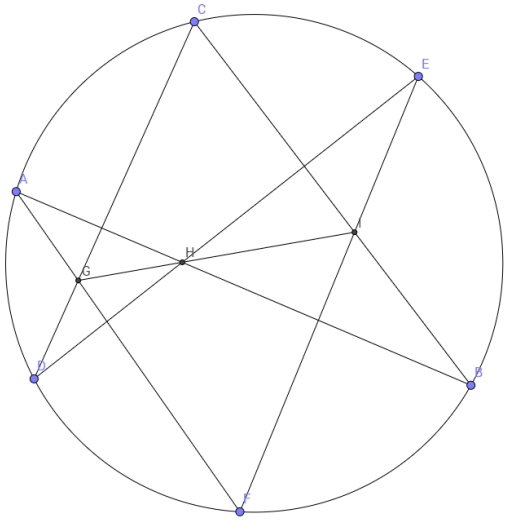
Course by Daniil Rudenko.

We will start with projective geometry, and then add algebra to it. No schemes in this course, we will be closer to the 19th century stuff. We are not following any particular book(s). Number one book is "Algebraic Geometry" by Shafarevich, our goal is all of chapter 1. We will start with projective geometry, a book for that is Prasolov (roughly).

1 Projective Geometry

1.1 Lecture 1

Algebraic geometry studies solutions to systems of algebraic equations/algebraic curves (which are loci of solutions of algebraic equations). One of the most famous renaissance geometry results is the Pascal theorem: the points G, H, I in the diagram below are colinear for any configuration of A, B, C, D, E, F on the circle.



A similar result to that is Pappus' theorem. Another top theorem is by Cayley-Salman 1849: A smooth projective cubic surface contains exactly 27 lines. Another such theorem is that any smooth projective curve of degree 4 has 28 bitangent lines (tangent in exactly two points). Working toward proofs of these results using algebraic geometry is our goal.

History of the subject: throughout the 19th century it developed very quickly, people who were into Euclidean geometry just transitioned to algebraic geometry and discover miracles like we described above. During the late 19th century Italians, who before led algebraic geometry, started producing very incorrect results because the technical aspects became too hard. Oscar Zariski and others saved the subject by rigorizing it using commutative algebra, with the language of ideals and rings, etc. We will see some 'wrong' arguments by the Italian school and see why they are not precise enough. There was another revolution by Grothendieck and the Bourbaki group in developing the language of schemes, which we will not touch in this course ("You will need to sacrifice a year of your life to start speaking that language. I never needed to, but a lot of people do.")

(Rudenko plug: woollymathematics.com)

Take $\mathbf{F}$ to be some field (usually $\mathbb{C}$), and polynomials $p_1, \ldots, p_k \in \mathbf{F}[x_1, \ldots, x_n]$, and study the solutions to the system

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ p_k(x_1, \ldots, x_n) = 0 \end{cases}$$

Fact 1. *If $k = 1$ and $p_1(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ for $d \geq 1$, $p_1(x) = 0$ has $\leq d$ solutions in $\mathbf{F}$.*

If $k = 2$, the number of solutions is $\leq$ than the product of the degrees of the polynomials. Of course we usually want a precise number of solutions, but generally we can't hope for anything more than upper bounds.

Fact 2. *If $\mathbf{F} = \mathbb{C}$, then $p(x) = 0$ has a solution.*

This is a remarkably hard result called the Fundamental Theorem of Algebra. There is a result that is in a way easier:

Fact 3. *If $\mathbf{F} = \mathbb{C}$, then $p(x) = 0$ has exactly d solutions if counted with multiplicity.*

We would hope for something like that but for $k > 1$. Bezout's theorem kind of satisfies that, but the picture is more complicated. For example, take a line and a hyperbola. While we would expect 4 solutions up to multiplicity, but take a line intersecting one of the components of the hyperbola transversally that is parallel to one of the other component's asymptotes. However, everything becomes nicer if we change the complex plane to the projective plane. The study of geometry on the projective plane is the projective geometry, and that's what we will study first.

Definition 1. *Let $\mathbf{F}$ be a field. A **projective space** $\mathbb{P}^n_{\mathbf{F}}$ is the set of lines in the vector space $\mathbf{F}^{n+1}$.*

An example for $\mathbf{F} = \mathbb{R}$, $\mathbb{P}^2_{\mathbb{R}}$ is the set of lines through the origin in the real plane. We can think of $\mathbb{P}^1_{\mathbb{R}}$ as all the points of a line in $\mathbb{R}^2$ not through the origin (say the line $y = 1$ in $\mathbb{R}^2$) but with a point at infinity added.

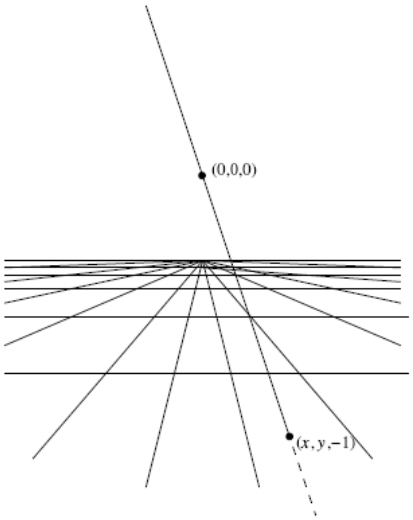
In $\mathbb{R}^2$, usually two lines intersect at one point, and two points are contained in one line. We can also define $\mathbb{P}^2_{\mathbb{R}}$ as the set of points of $\mathbb{R}^2$, and the set $[l]$ (points at ∞), which are equivalence classes of lines in $\mathbb{R}^2$ by $l_1 \sim l_2$ for l_1 and l_2 are parallel. Note that there is one more line, line at infinity, consisting only of points $[l]$.

Fact 4. *In $\mathbb{P}^2_{\mathbb{R}}$ every two distinct lines intersect in one point and every two points are contained in precisely one line.*

Proof. Non-parallel lines intersect in the usual way. Parallel lines intersect at their equivalence class $[l]$. If one of the lines is the 'line at infinity', they intersect at the equivalence class of the other line. Similarly we can examine the second part of the statement. □

Fact 5. *For $\mathbb{P}^2_{\mathbb{R}}$, the abstract definition 1 is equivalent to the definition we gave in the example.*

Proof. Take a plane in $\mathbb{R}^3$ not passing through the origin, $z = -1$ for example. Then we can create a bijection between the set of lines through the origin and the set of points on the plane and the set of points at infinity, by mapping the lines that intersect the plane with their intersection point, and those that are parallel with the plane to their equivalence class on the plane $\mathbb{R}^2$. Thus we have a bijection between the two objects we defined.



□

Another way to think of $\mathbb{P}^2_{\mathbb{R}}$ is as a sphere with antipodal points identified.
"ChatGPT can make you Snake 4: Snake but on the projective plane."

1.2 Lecture 2

A **geometry** is a set X along with a group G acting on X, $x \mapsto gx$, which defines 'equivalences' between subsets of X.

Example 1.
- *Let $X = \mathbb{R}^2$, G the group of **isometries**: distance preserving bijections. Indeed, isometries also preserve lengths, areas, angles, etc. Think of them as congruences in Euclidean geometry.*

- *Let X be a vector space, $G = GL(V)$, the general linear group. More specifically, let $X = F^n$ for some field G, then $G = \mathrm{GL}_n(F)$.*

Definition 2. *Fix F some field. Define **affine space** $\mathbb{A}^n_F = F^n$, with the group of **affine transformations***

$$\mathrm{Aff}_n = \{f : \mathbb{A}^n \to \mathbb{A}^n \mid f(x) = Ax + b, A \in \mathrm{GL}_n(F), b \in A^n\}$$

A typical way of thinking about affine space is as a vector space without a fixed origin.

Example 2. *Circles don't make much sense in $\mathbb{A}^2_{\mathbb{R}}$ anymore, since $x^2 + y^2 = 1$ is equivalent to an ellipse (say by $(x, y) \mapsto (2x, 5y)$).*

Definition 3. *An **affine algebraic variety** is a set of solutions of a system of polynomials $P_1, \ldots, P_k \in F[x_1, \ldots, x_n]$:*

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ P_k(x_1, \ldots, x_n) = 0 \end{cases}$$

Example 3.
- *$P_1(x, y) = 2x + y - 1 = 0$ gives a line; $P_1(x, y) = x^2 + y^2 - 1 = 0$ gives a circle.*
- *$P_1(x, y, z) = 2x + y - z - 1 = 0$ and $P_2(x, y, z) = x + y - 3 = 0$, then the variety is an intersection of two planes, thus a line.*

If $P_1, \ldots, P_k$ are linear $\sum a_i x_i + b$ then we will call it **affine subspace**.

We can identify pairs of points in $\mathbb{A}^n$ with vectors in a vector space F^n, where vectors $\overrightarrow{AB}$ are pairs of points (A, B), identified via the equivalence relation $\overrightarrow{A_1B_1} \sim \overrightarrow{A_2B_2}$ iff $(A_1)_i - (B_1)_i = (A_2)_i - (B_2)_i$. An observation is that if $f : \mathbb{A}^n \to \mathbb{A}^n$ is an affine transformation, then $f(\overrightarrow{AB}) = \overrightarrow{f(A)f(B)}$.

What we just described is a homomorphism $\mathrm{Aff}_n \to \mathrm{GL}_n$ which maps $f = Ax + b$ to $A \in \mathrm{GL}_n$. The kernel of this map is isomorphic to $\mathbf{F}^n$ as an additive group.

Definition 4. *If $A_1, \ldots, A_{n+1} \in \mathbb{A}^n$ are in **general position** if $\overrightarrow{A_1A_i}$ for $i = 2, 3, \ldots n + 1$ are all linearly independent. Equivalently (exercise) $A_1, \ldots, A_{n+1}$ are not in the same affine hyperplane.*

Theorem 1. *Suppose $A_1, \ldots, A_{n+1} \in \mathbb{A}^n$ and $B_1, \ldots, B_n \in \mathbb{A}^n$ are points in general position in $\mathbb{A}^n$. Then there is a unique $f \in \mathrm{Aff}_n$ s.t. $f(A_i) = B_i$ for each i.*

Proof sketch: Using translation by a vector $\overrightarrow{A_1B_1}$, move A_1 to B_1. This reduces this problem to the uniqueness of a linear transformation from the basis $\overrightarrow{A_1A_i} \to \overrightarrow{B_1B_i}$. □

Observation: "X is the midpoint of the segment $\overline{A_1A_2}$" is an affine property: $f(X)$ is still the midpoint of $\overline{f(A_1)f(A_2)}$. Application of this:

Theorem 2. *Three medians of a triangle intersect at a point.*

Proof. Let ABC be an arbitrary triangle in $\mathbb{A}^2_{\mathbb{R}}$. Let f be the affine transformation taking an equilateral triangle to ABC. The medians of an equilateral triangle intersect at a point by symmetry. But medians get sent to medians, and intersections are preserved, so the medians of ABC must intersect also. □

Definition 5. *Let V be a vector space over F, then its **projectivization** $\mathbb{P}(V)$ is the set of lines (1-dim vector subspaces) in V.*

By definition the dimension of $\mathbb{P}(V)$ is $\dim V - 1$. If $V = F^{n+1}$, $\mathbb{P}(V) = \mathbb{P}^n_F$. More explicitly, $\mathbb{P}(V) = (V - \{0\})/(v \sim \lambda v, \lambda \in F)$. We express points in $\mathbb{P}(V)$ by **homogeneous coordinates** so $[X_0 : X_1 : \cdots : X_n]$, with the aforemetioned equivalence relation (so e.g. $[0, 1, 0] = [0, 2, 0]$)

"Gold to silver to whiskey, the ratio should be 1 to 1 to 100. You're making a cocktail. Don't do that by the way... Point of projective geometry is to make cocktails."

If $A = [X_0 : \cdots : X_n] \in \mathbb{P}^n$. If $X_n \neq 0$ then $A = [X_0/X_n : \cdots : X_{n-1}/X_n, 1]$, points of this form this are in bijection with $\mathbb{A}^n$. Indeed, $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0$. The points with $X_n = 0$ are in bijection with points in $\mathbb{P}^n$ (divide all entrees by the first non-zero entry from the right). For example, $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R} \cup \infty$, where $\mathbb{R}$ is in bijection with points $[X_0/X_1 : 1]$ and ∞ represents $[1 : 0]$.

Barycentric coordinates are basically the same thing as homogeneous coordinates but in a different language. Imagine putting masses m_1, m_2, m_3 at the vertices of a triangle, then look at their center of mass. If $m_1 = m_2 = m_3$ then this point is the centroid. More precisely, if O is any point, we have that the point M with homogeneous coordinates (m_1, m_2, m_3), the center of mass for some m_1, m_2, m_3 (sum non-zero), is such that

$$\overrightarrow{OM} = \frac{m_1\overrightarrow{OA_1} + m_2\overrightarrow{OA_2} + m_3\overrightarrow{OA_3}}{m_1 + m_2 + m_3}$$

As such, O has homogeneous coordinates $(m_1 : m_2 : m_3)$ in the projective plane.

A homogeneous polynomial is one where each term has the same degree. Then it makes sense to talk about $P([x_0, \ldots, x_d]) = 0$ for a homogeneous polynomial P, since such polynomials respect the equivalence relation of homogeneous coordinates.

Definition 6. ***Projective variety** is a subset of $\mathbb{P}^n_F$ which is the set of solutions of a system:*

$$\begin{cases} P_1([X_0 : \cdots : X_n]) = 0 \\ \vdots \\ P_k([X_0 : \cdots : X_n]) = 0 \end{cases}$$

where each P_i is homogeneous.

Example 4. *Say $P(x, y, z)y - x^2$, which we can think of as points $[x : y : 1]$ that satisfy the parabola. We can relabel $[x : y : 1]$ into $[X : Y : Z]$ with $x = X/Z, y = Y/Z$, so the set of points satisfying $P_1([X : Y : Z])$ is the set such that $X^2 = YZ$. So for instance $[0 : 1 : 0]$ is also a solution. We can think of this as the parabola becoming an ellipse because it closes at infinity.*

1.3 Lecture 3

Observation: If we have an injective linear map $f : V_1 \to V_2$, and L is a line in V_1, then $f(L)$ is also a line. So, f induces a map $\overline{f} : \mathbb{P}(V_1) \to \mathbb{P}(V_2)$.

Definition 7. *If $V_1 = V_2$ in the above, then the set of maps $\mathbb{P}(V) \to \mathbb{P}(V)$ induced by linear maps $V \to V$ form the* ***projective linear group*** $\mathrm{PGL}(V)$. *If $V = \mathbf{F}^n$, we denote $\mathrm{PGL}(V) = \mathrm{PGL}_n(\mathbf{F})$.*

$\mathrm{PGL}_n(F)$ has a simple description: Let $\Phi : \mathrm{GL}_n(\mathbf{F}) \to \mathrm{PGL}_n(\mathbf{F})$ be defined by $f \to \overline{f}$. Then $\ker \Phi$ is the set of all diagonal matrices (since those are identity on one-dim spaces), which is isomorphic to $F^\times$. So, $\mathrm{PGL}_n(\mathbf{F}) = \mathrm{GL}_n/F^\times$ by first isomorphism theorem.

Now consider $\mathbb{P}^1_{\mathbf{F}}$, and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_n(\mathbf{F})$. Then $\overline{f}([x : y]) = [ax + by : cx + dy]$. Note that we can interpret $\mathbb{P}^1_{\mathbf{F}} = \mathbb{A}^1_{\mathbf{F}} \cup \infty$, where $A^1_{\mathbf{F}}$ can be thought of as the set of all $[x : 1]$, and ∞ can be thought of as $[0 : 1]$. So on $\mathbb{A}^1_{\mathbf{F}}$, $[ax + by : cx + dy] = [\frac{ax+b}{cx+d} : 1]$. So on the affine line, $\overline{f}$ sends x to $\frac{ax+b}{cx+d}$.

If $f(x) = 1/x$, then $[x : y] = [x/y : 1]$ gets sent to $[y/x : 1] = [y : x]$ by $\overline{f}$. Hence, $[0 : 1] \mapsto [1 : 0]$, or in other words $0 \mapsto \infty$ in $\mathbb{P}^1_{\mathbf{F}}$. This corresponds to the analytic intuition: as x gets closer to 0, $1/x$ gets closer to infinity.

Now look at $\mathbb{P}^2_{\mathbf{F}}$, and consider the linear transformation

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$\overline{A}$ sends $[x_1 : x_2 : x_3]$ to $[a_{11}x_1 + a_{12}x_2 + a_{13}x_3 : \dots]$. So, as a map on $\mathbb{A}^2_F$,

$$\overline{A}(u, v) = \left(\frac{a_{11}x_1 + a_{12}x_2 + a_{13}x_3}{a_{31}x_1 + a_{32}x_2 + a_{33}x_3}, \frac{a_{11}x_1 + a_{12}x_2 + a_{13}x_3}{a_{31}x_1 + a_{32}x_2 + a_{33}x_3} \right)$$

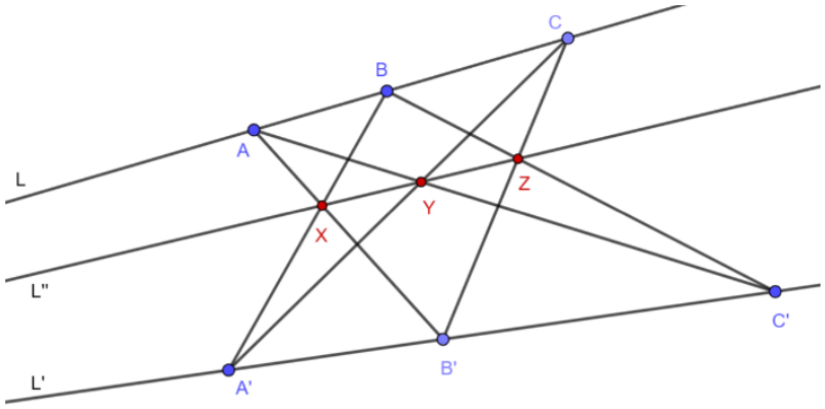
"If you have a dictator you don't like and you want to get rid of them, you can just take a projective transformation of them and send them to infinity. That's what they used to do with dictators."

By this he means, by choosing the last row of A appropriately, we can get $\overline{A}$ to send any given line in $\mathbb{A}^2_{\mathbf{F}}$ to infinity.

Theorem 3. *Consider points $A_1, \dots A_{n+2}$, $B_1, \dots, B_{n+2}$ in $\mathbb{P}^n$ such that $\{A_i\}$ and $\{B_i\}$ are in general position (on $\mathbb{P}^n$ this means for any i, $A_1, \dots, \hat{A}_i, \dots, A_{n+2}$ span F^{n+1} when considered as vectors in F^{n+1}). Then there exists $\overline{f} \in \mathrm{PGL}_n(\mathbf{F})$ such that $\overline{f}(A_j) = B_j$ for $1 \le j \le n + 2$.*

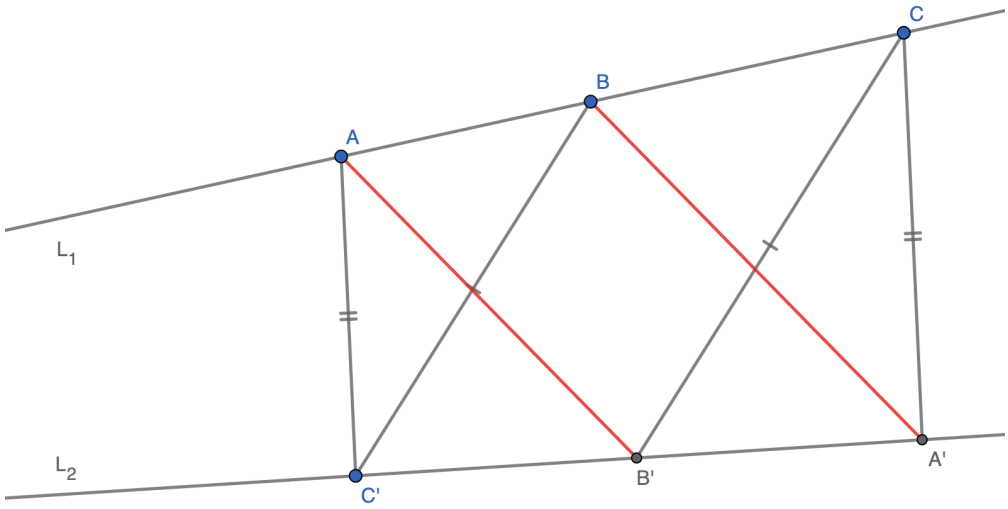
Proof. Let $A_i = [v_i]$, $B_i = [w_i]$, where $[v_i]$ is the equivalence class of some vector $v_i \in \mathbf{F}^{n+1}$. Then by assumption $v_1, \dots, v_{n+1}$ and $w_1, \dots, w_{n+1}$ are bases of F^{n+1}, so there exists a unique linear transformation f_1 such that $f_1(v_i) = w_i$. Then, $f_1(v_{n+2}) = \tilde{v}_{n+2}$. Since $v_{n+2} = \lambda_1 v_1 + \dots + \lambda_{n+1} v_{n+1}$, this maps to $\tilde{v}_{n+2} = \lambda_1 w_1 + \dots \lambda_{n+1} w_{n+1}$. Also $w_{n+2} = \mu_1 w_1 + \dots + \mu_{n+1} w_{n+1}$. Note that this means $\lambda_i, \mu_i \neq 0$ for any i. Then, let f_2 be a linear map sending w_i to $\frac{\mu_i}{\lambda_i} w_i$ so $f_2 \circ f_1(v_1) = \frac{\mu_1}{\lambda_i} w_i$ and $f_2 \circ f_1(v_{n+2}) = w_{n+2}$. As such, $\overline{f_2 f_1}$ sends A_i to B_i. Uniqueness is left as an exercise. $\square$

Theorem 4 (Pappus' Theorem)**.** *Consider the diagram*



The points X, Y, Z are always colinear. [Note: the diagram he drew in class had points labelled differently, I changed them because this diagram is from the internet.]

Proof. Take the line through Y and Z, send it via a projective transformation to the line at infinity. Then, to show X is on the same line as Y, Z it suffices to show that after the transformation $\overline{AB'}$ is parallel to $\overline{A'B}$ (marked red in the diagram below:)



This is true by angle chasing using the parallel line postulate. □

For $\mathbb{P}^1$, recall that $\mathrm{PGL}_2(\mathbf{F}) = \{\frac{ax+b}{cx+d} \mid ad - bc \neq 0\}$. By the theorem above, elements of $\mathrm{PGL}_2(\mathbf{F})$ send any three distinct points to any three distinct points. This is not true however for four points, so it makes sense that there would be some sort of invariant associated with four points.

Definition 8. *If $x_1, x_2, x_3, x_4 \in \mathbb{P}^1$ are distinct, **cross ratio** of these points is defined*

$$[x_1, x_2, x_3, x_4] = \frac{(x_1 - x_2)(x_3 - x_4)}{(x_1 - x_4)(x_3 - x_2)}$$

If $x_4 = \infty$,

$$[x_1, x_2, x_3, \infty] = \frac{x_1 - x_2}{x_3 - x_2}$$

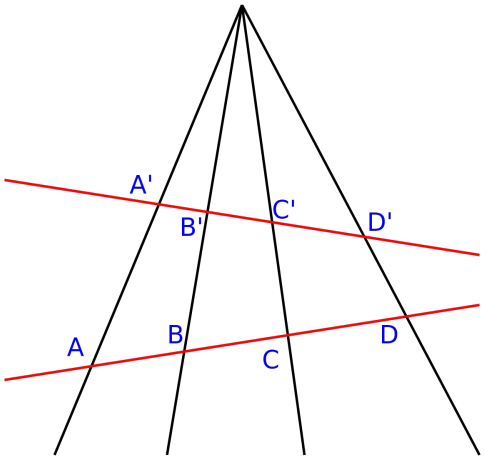
Similarly define for any other $x_i = \infty$.

Theorem 5. *If* $f \in \mathrm{PGL}_2(\mathbf{F})$ *then* $[f(x_1), f(x_2), f(x_3), f(x_4)] = [x_1, x_2, x_3, x_4]$. *So, cross ratio is an invariant of* $\mathrm{PGL}_2(\mathbf{F})$.

Proof. $\mathrm{PGL}_2(\mathbf{F})$ as a group is generated by the following transformations: $x \mapsto x+b$, $x \mapsto ax$, $x \mapsto 1/x$. It is easy to see that the first two leave cross ratio unchanged. The third is an algebra bash. □

Note that $[x_1, x_2, x_3, x_4] = [x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}]$ for $\sigma \in K$, the Klein 4-group in S_4, so in fact $\sigma \in S_4$ can only change $[x_1, x_2, x_3, x_4]$ into $\lambda, 1-\lambda, 1/\lambda, 1-1/\lambda, \lambda/(\lambda-1), 1/(1-\lambda)$. Proving this will be an exercise.

Proposition 1. *Let* $l_1, l_2 \in \mathbb{P}^2$, $O \in \mathbb{P}^2$ *not on* l_1 *or* l_2. *Consider a projection of* l_1 *onto* l_2 *about* O, *as in the diagram (with* O *unlabelled on top):*



More precisely, if $A' \in l_1$ *and* $\overrightarrow{OA'}$ *is a line in* $\mathbb{P}^2$ *containing both* O *and* A', *this map is* $A' \mapsto A = \overrightarrow{OA'} \cap l_2$. *This is a projective transformation.*

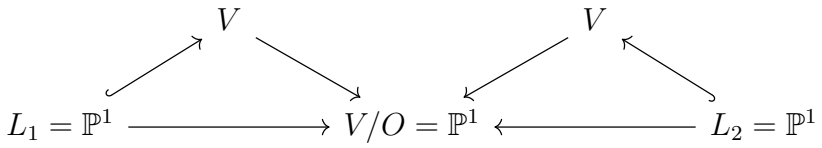
Note that using this diagram, the invariance of cross ratio can be interpreted as the equivalence of ratios segments, as such:

$$\frac{|C'A'|}{|C'B'|} : \frac{|D'A'|}{|D'B'|} = \frac{|CA|}{|CB|} : \frac{|DA|}{|DB|}$$

[A proof of this equality with elementary trigonometry is in Prasolov]

Proof. Let L_1, L_2 be planes and O be a line in $V = \mathbf{F}^3$ not contained in either plane. Take the plane V/O, then $\mathbb{P}(V/O) = \mathbb{P}^1$. Then $L_i \to V \to V/O$, the composition of inclusion and

quotient, gives us a map $\mathbb{P}^1 \to \mathbb{P}^1$. Indeed, we have the commutative diagram



With the bottom two arrows being isomorphisms. Composing the left arrow with the inverse of the right arrow gives us a map in $\mathrm{GL}_2(F)$ between L_1 and L_2, which induces the projection map in $\mathrm{PGL}_2(F)$. □

1.4 Lecture 4

(OH 5PM)

[TODO: there are some errors in this lecture]

Recall: We consider a field $\mathbf{F}$, mostly $\mathbb{R}, \mathbb{C}$ or $\mathbf{F}_p$. As we defined before, $\mathbb{P}^n_{\mathbf{F}} = (\mathbf{F}^{n+1} \setminus 0)/\mathbf{F}^\times$, where the identification is $(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n)$. An equivalence class like this is denotes via homogeneous coordinates $[x_0 : \cdots : x_n]$. We can identify the affine plane $\mathbb{A}^n_{\mathbf{F}}$ by considering the set of points with $x_n \neq 0$ (i.e. by excluding the lines at infinity).

Note we may write $R = \mathbf{F}[x_0, \ldots, x_n] = R_1 \oplus R_2 \oplus \ldots$ where R_d is a vector space of homogeneous polynomials with degree of terms being d (so $x_0^{k_0} x_1^{k_1} \ldots x_n^{k_n}$ with $\sum k_i = d$). R_0 is the base field. R_1 is the dual space V^* of $\mathbf{F}^n$ (since all homog. polys of deg 1 are precisely all linear maps). $R_2 = \mathbb{S}^2 V^*$, and in general $R_d = \mathbb{S}^d V^*$.

Definition 9. *Let $F \in R_d$ be a homog. polynomial with $d \neq 0$. Then the set of solutions of an equation $F(x_0, \ldots, x_n) = 0$ is called a **hypersurface** of degree d in $\mathbb{P}^n$.*

Example 5. *In $\mathbb{P}^3$, $x_0^3 - x_1^3 + x_2 x_3^2 + x_3^3 = 0$. The intersection of this with $\mathbb{A}^3$ (obtained by dividing all terms by x_3) we get $(x_0/x_3)^3 - (x_1/x_3)^3 + x_2/x_3 + 1 = 0$. The rest of this hypersurface is in $\mathbb{P}^3 \setminus \mathbb{A}^3 = H$, it is defined by $x_0^3 - x_1^3 = 0$. Since $H \cong \mathbb{P}^2$, we can do the same procedure to reduce this hypersurface to something we can draw in $\mathbb{A}^2$, getting $y_0^3 - y_1^3 = 0$, which are three lines intersecting at the origin (if $\mathbf{F} = \mathbb{C}$). Going the other way from $y_0^3 + y_1^3 + y_2 + 1 = 0$ by introducing another variable and going into $\mathbb{P}^3$ is called homogenization.*

Definition 10. *A **projective variety** is a finite intersection of hypersurfaces.*

(Note: you do not get more sets if you extend this to an infinite system, by the Hilbert basis theorem, to be covered later).

Definition 11. *A hypersurface $X = \{F = 0\}$ for $F \in R_d$ is **irreducible** precisely when F is irreducible.*

Example 6.

- *$x_0 x_1 = 0$ in $\mathbb{P}^2$ is a union of two lines. Not irreducible polynomial, so the hypersurface is not irreducible also. In general, any union of two lines is not irreducible.*
- *$x_0^2 + x_1^2 = x_2^2$ is irreducible, so its hypersurface, a circle in $\mathbb{A}^2$.*

Assume $\mathbf{F} = \mathbb{C}$. Consider the action of PGL_{n+1} on degree d hypersurfaces in $\mathbb{P}^n$. Take $d = 1$, then this action is transitive, as we saw last time. Thus up to projective transformations all hyperplanes are the same. If $d = 2$, F looks like

$$\sum a_{ij} x_i x_j = (x_0, \ldots, x_n) A \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = x^\top A x$$

Subject to a projective transformation, $x = Uy$ for some $y \in \mathbb{P}^n$. Thus, $x^\top A x \mapsto y^\top U^\top A U y = 0$.

Theorem 6. *Any quadric is a projectively equivalent to a quadric* $\lambda_0 x_0^2 + \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 = 0$

[TODO: This is equivalent to (some) matrix diagonalization result, didn't catch which one that was.] Exercise: prove this my hand for $n = 2$.

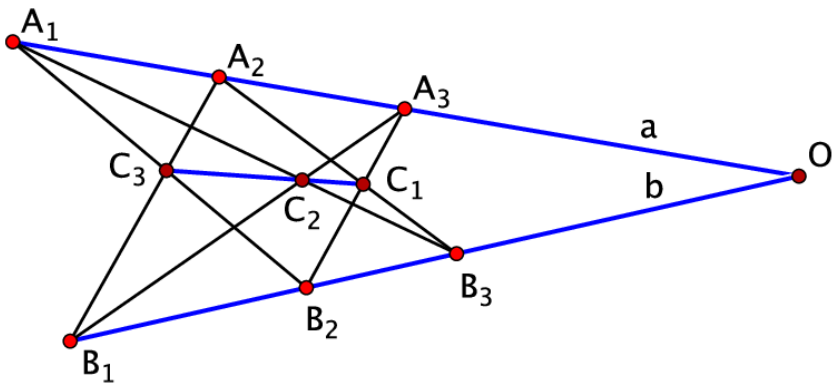
So, if $\mathbf{F} = \mathbb{R}$, for $n = 2$ the picture is complicated, for example $x_0^2 - x_1^2 - x_2^2 = 0$ is a double cone. But for $\mathbf{F} = \mathbb{C}$ things become simpler because everything can be reduced to the cases $x_0^2 + x_1^2 + \cdots + x_i^2 = 0$. So in $\mathbb{P}^2_{\mathbb{C}}$ we have lines, intersections of two lines, and conics, for $i = 1, 2, 3$ respectively. Thus the action of PGL_3 has three orbits, namely those classes.

Now we discuss projective duality. Suppose we are working in $\mathbb{P}^2$. A line here is defined by an equation $ax + by + cz = 0$ with not all $a, b, c = 0$, modulo rescaling. Thus lines in $\mathbb{P}^2$ also form a projective space. This has some striking applications.

Conceptually, if we have $\mathbb{P}^n = \mathbb{P}(V)$ for an n-dim vector space V, hyperplanes in $\mathbb{P}^n$ are in bijection with the elements of $\mathbb{P}(R_1) = \mathbb{P}(V^*)$.

The **duality principle** can be stated as follows. Consider any theorem about points and lines in $\mathbb{P}^2$, replacing lines by points and vice versa gives another valid theorem.

Example 7. *Recall Pappus' theorem. The dual to this theorem can be drawn as follows: (TODO: wrong diagram)*



The statement is that lines a, b, and c (passing through C_i) all pass through O.

In a dualization of a theorem, for every line there is a point, for every point there is a line. If n lines intersect at a point, in the dual theorem n points will lie on one line.

In $\mathbb{P}^3$ a similar duality holds: points correspond to planes, lines correspond to lines, planes correspond to points.

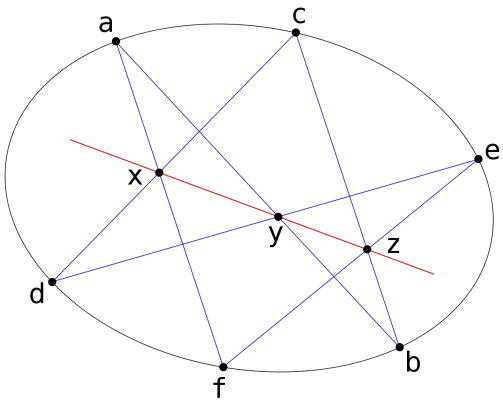
Three important facts about V^*: 1. $\dim V = \dim V^*$ since V and V^* are (not canonically) isomorphic, 2. $V \cong (V^*)^*$ canonically via an isomorphism $v \mapsto (\phi : V \to F \mapsto \phi(v))$, 3. There is an inclusion reversing bijection between subspaces of V and V^*, which is equivalent to $\dim W + \dim W^\top = \dim V$.

1.5 Lecture 5

Let's talk about conics a little bit more. If $\mathbb{P}^n_{\mathbf{F}} = \mathbb{P}(\mathbf{F}^{n+1})$, so $[x_0 : x_1 : \cdots : x_n]$ are homogeneous coordinates on $\mathbb{P}^n_{\mathbf{F}}$, and $P(x_0, \ldots, x_n)$ is a homogeneous polynomial of degree d, $\{[x_0, \ldots, x_n] \mid P(x_0, \ldots, x_{n+1}) = 0\} \subset \mathbb{P}^n$ is a hypersurface of degree d. For $d = 1$ this is the familiar hyperplane. If $d = 2$ this is a *quadric*.

Over $\mathbb{C}$ (polynomials with coeffs in $\mathbb{C}$), every quadric is either a union of two lines, a cross of two lines, or a conic (which are all the same on the projective plane). The conic is called the *smooth* quadric.

Theorem 7 (Pascal)**.**



For any ellipse, putting distinct A, B, C, D, E, F on it and connecting them a la Pappus' theorem gives us colinear intersection points X, Y, Z.

"Who thinks this is beautiful? If you don't [points to door]"

In this way Pappus' theorem is not surprising because both a pair of lines and a conic are quadrics over $\mathbb{C}$.

Lemma 1 (Chasles)**.** *Let points A_1, A_2, A_3, A_4 and X, Y lie on a conic. Then*

$$[(XA_1), (XA_2), (XA_3), (XA_4)] = [(YA_1), (YA_2), (YA_3), (YA_4)]$$

Notice that there is a bijection between points of a conic and lines through some particular point X on a conic C. Indeed, a line through X is either tangent to the conic or intersects it at some other point. Associating the tangent line to X and the other lines to their intersection points, we associate the points of C with $\mathbb{P}^1$. Indeed, the result above follows by using the two bijections onto $\mathbb{P}_1$ given by X and Y, and concluding that there is a projective transformation mapping the X configuration to the Y configuration. This however requires some details we haven't gone over, so below is an elementary proof:

Proof. (TODO: diagram) First, assume the conic C is a circle in $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$. If the points are ordered $A_1, \ldots, A_4$ from left to right, let U and V be intersection points of a line A_1A_4 through XA_2, XA_3. Then

$$[XA_1, \ldots, XA_4] := [X_1, U, V, X_4] = \pm \frac{S_{A_1XY} S_{VXA_1}}{S_{A_1XA_2} S_{UXV}} = \frac{\sin \angle X_1XU \sin \angle VXA_1}{\sin \angle A_1XA_2 \sin \angle UXV}$$

where S_{ABC} is the notation for the area of triangle ABC. But by [these angles from X and Y are called something I forget what], we know that they remain invariant if we replace X with Y. We thus have shown that the cross ratio remains the same. □

Proof: (Of Pascal's). By the lemma above,

$$[A_1B_1, A_1B_2, A_1B_3, A_1A_2] = [A_3B_1, A_3B_2, A_3B_3, A_3A_2]$$

Now label the two intersection points above the line XYZ in the diagram S and T. Then by definition of cross ratio of four lines,

$$[B, Z, S, A_2] = [T, X, B_3, A_2]$$

by picking the transversal line to be A_2B_1 and A_2B_3 for the left and right cross ratios respectively. But this quantity is also equal to $[(B_1Y), (ZY), (SY), (A_2Y)]$. We want X and Z to be colinear with Y, let X' be the intersection of the line ZY with A_2B_3. Then,

$$[(B_1Y), (ZY), (SY), (A_2Y)] = [T, X', B_3, A_2] = [T, X, B_3, A_2]$$

This implies $X = X'$, which concludes the proof. □

Our goal now is to go towards Bezout's theorem. The statement of the theorem is as follows: In $\mathbb{P}^2_{\mathbb{C}}$ let X and Y be projective curves such that they do not have common irreducible components. Then the number of points in their intersection is less than or equal to the product of their degrees, and in fact (hard part) is *equal* up to multiplicity. Of course, it's hard because it's hard to define exactly what 'up to multiplicity' means. Take two concentric circles $x^2 + y^2 = 1$ and $x^2 + y^2 = 2$ in $\mathbb{A}^2$. These only have solutions once you homogenize them and pass over to the complex projective plane. Then, $x^2 + y^2 = z^2, x^2 + y^2 + 2z^2$ have solutions $[1 : i : 0], [1 : -i : 0]$. By Bezout's these points have to have intersection multiplicty 2, so in fact they are *tangent points*.

For now, we will only prove the easier upper bound on the number of intersection points.

Theorem 8 (Sylvester)**.** *Let $A(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots a_0 = 0$ and $B(x)$ be polynomials of degree m and n respectively. They have a common factor of degree ≥ 1 if and only if the following $(m+n) \times (m+n)$ matrix*

$$\begin{bmatrix}
a_m & a_{m-1} & \ldots & a_0 & 0 & \ldots & 0 \\
0 & a_m & \ldots & a_1 & a_0 & \ldots & 0 \\
 & & \vdots & & & & \\
0 & 0 & \ldots & a_m & \ldots & & a_0 \\
b_n & b_{n-1} & \ldots & & b_0 & \ldots & 0 \\
0 & b_n & \ldots & & & \ldots & 0 \\
 & & \vdots & & & & \\
0 & 0 & \ldots b_n & & \ldots & & b_0
\end{bmatrix}$$

(where a_i appear in the first n rows, b_j appear in the last m rows) has determinant 0. *The determinant is called the* ***resultant*** *of A and B.*

Proof. A and B have a common factor iff there exist non-zero polynomials U and V of degrees less than n and m respectively, such that $A \cdot U = B \cdot V$. This is a linear combination in the first n rows being equal to a linear combination of the last m rows, hence this condition holds iff $\det = 0$. □

You can use this theorem to solve systems of polynomial equations by eliminating a variable, writing the condition that there is a solution in terms of the resultant. This is highly impractical if the degrees of equations are large, but is a useful proof technique.

1.6 Lecture 6

Note that to generalize Sylvester's theorem to also work for polynomials over a ring and not a field we need to use Gauss' lemma.

Theorem 9. *Suppose that $f(x) = a_m(x - t_1)\dots(x - t_m)$, and $g(x) = b_n(x - s_1)\dots(x - s_n)$. Then their resultant is*

$$\operatorname{Res}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (t_i - s_j)$$

Proof. Let's view $\operatorname{Res}(f, g)$ as a polynomial in $\mathbb{Z}[a_m, b_n, t_1, \dots, t_m, s_1, \dots, s_n]$ (can do by Vieta's formulas). Looking at the resultant matrix, we can extract an a_m and b_n from every row of the determinant, we get $\operatorname{Res} = a_m^n b_n^m P(t_1, \dots, t_m, s_1, \dots, s_n)$.

Now we mention a little trick: for $f(x)$ with coefficients in a unique factorization domain, $f(x_0) = 0$ iff $(x - x_0)$ divides $f(x)$. Indeed, take $\tilde{f}(x) = f(x + x_0) = \tilde{a}_n x^n + \dots + \tilde{a}_0$. But then $f(x) = \tilde{a}_n(x - x_0)^n + \dots + \tilde{a}_0$, which $(x - x_0)$ divides if and only if $\tilde{a}_0 = 0$, i.e. x_0 is a root.

Thus, P is divisible by $(t_i - s_j)$, since considering P as a polynomial with coefficeints in $\mathbb{Z}[t_1, \dots, \hat{t}_i, \dots, t_m, s_1, \dots]$. Thus, $P(s_j) = 0$ implies $(t_i - s_j) \mid P$. Note that $(t_i - s_j)$ are pairwise coprime, as such

$$\operatorname{Res}(f, g) = C a_m^n b_n^m \prod \prod (t_i - s_j)$$

Note that the product $\prod\prod(t_i - s_j)$ has the same degree nm as $\operatorname{Res}(f, g)$ (exercise), so by plugging in a point we realize $C = 1$. □

(Discriminants, Resultants, and Multidimensional Determinants - very underrated book)

Theorem 10 (Weak Bezout)**.** *Let F be an infinite field, consider two curves with no common irreducible components in $\mathbb{P}^2_{\mathbf{F}}$, defined by $P(X, Y, Z) = 0$, $Q(X, Y, Z) = 0$ with P and Q homogeneous (no common irreducible components means P and Q are coprime). Then, P and Q have at most* $\deg P \deg Q$ *solutions.*

Proof. Let $\deg P = m$, $\deg Q = n$. Assume the system $\{P = 0, Q = 0\}$ has $nm+1$ solutions of the form (X_i, Y_i, Z_i). Note there exists a coordinate system such that **1**. P and Q are not divisible by Z and **2**. $Z_i \neq 0$ **3**. $\frac{Y_1}{Z_1}, \ldots, \frac{Y_{n+m}}{Z_{n+m}}$. Then we have $f(x,y) = \frac{P(X,Y,Z)}{Z^m}$, $g(x,y) = \frac{Q(X,Y,Z)}{Z^n}$ are polynomials of degree m and n respectively in X/Z, Y/Z. They also have $nm+1$ solutions (x_i, y_i) with all y_i distinct, and f and g have no common factor of degree ≥ 1. Let's view $f(x,y), g(x,y)$ as polynomials in $(\mathbf{F}[y])[x]$. Note that $\operatorname{Res}(f,g)$, a polynomial in $\mathbf{F}[y]$, is nonzero with roots $y_i, \ldots, y_{nm+1}$. It remains to show that $\deg \operatorname{Res}(f,g) < nm$. Left as a (non-trivial) exercise. □

An application of this theorem. Suppose we are working in $\mathbb{P}^2_{\mathbb{C}} = \mathbb{P}(\mathbb{C}^3)$. Curves of degree 1 are lines, they form $\mathbb{P}(V^*) = \mathbb{P}^2$ as we have seen before. Curves of degree 2 of form $ax^2+bxy+cy^2+dxz+eyz+fz^2$ form a space $\mathbb{P}^5$ (one less than the coordinates). All degree 2 curves containing a point $[x_0, y_0, z_0]$ form a (4-dimensional) hyperplane in $\mathbb{P}^5$. Space of degree 2 curves containing 2 points P_1, P_2 will have dimension at least 3, but it can be 4. Degree 2 curves containing P_1, P_2, P_3 will have dimension at least 2, ... we thus can show that any 5 points in $\mathbb{P}^2$ lie on a curve of degree 2.

1.7 Lecture 7

Consider $\mathbb{P}^5 = \mathbb{P}(\mathbb{S}^2 V^*)$, the space of quadrics $F = a_1x^2+a_2xy+\cdots+a_6$ in $\mathbb{P}^2$, corresponding to the coordinate $[a_1 : a_2 \cdots : a_6]$. For a $P \in \mathbb{P}^2$, the set H_P of quadrics containing P forms a hyperplane in $\mathbb{P}^5$.

[The proof of this will probably be on the exam]

Theorem 11. *Let $P_1, \ldots, P_5 \in \mathbb{P}^2$ be points in general position (no three points lie on the same line). Then there exists a unique quadric containing $P_1, \ldots, P_5$.*

Proof. Consider $H_1 \cap \cdots \cap H_5$ in the space of quadrics $\mathbb{P}^5_{\mathbb{C}}$ (of dimension 6), need to show that this is precisely one point. Since intersecting hyperplanes drops dimensions by at most 1, we know that $H_{P_1} \cap \ldots H_{P_5}$ has dimension at least 1. Thus there is a quadric containing $P_1, \ldots, P_5$. Assume it is not unique, so C_1, C_2 are two distinct quadrics containing those points, as such $|C_1 \cap C_2| \geq 5$ which is impossible, say taking C_1, C_2 to be lines. (TODO: confused about dimensions. Are we considering $\mathbb{P}^5$ in $\mathbb{C}^6$?) □

[Reproducing this or something like it will be on the midterm]

Theorem 12 (Pascal's theorem on conic)**.** *Take $C = 0$ defining a conic, $A_1, \ldots, A_6$, $X = A_1A_5 \cap A_2A_4$, ... Then X, Y, Z lie on the same line. (TODO diagram, $A_1, \ldots, A_6$ go clockwise on ellipse)*

Proof. Let L_{UV} be the equation for the line through U, V. Consider curves $L_{A_6A_2}L_{A_5A_3}L_{A_1A_4}$ and $LA_1A_5L_{A_2A_4}L_{A_3A_6}$. These intersect at $A_1, \ldots, A_6, X, Y, Z$. For varying $\lambda \in \mathbb{C}$, consider the pencil of cubic curves $L_{A_6A_2}L_{A_5A_3}L_{A_1A_4} + \lambda LA_1A_5L_{A_2A_4}L_{A_3A_6}$ in $\mathbb{P}^9$ (projective space of cubic curves). Consider any point $P \in C$ that is not $A_1, \ldots, A_6$. Then there exists $\lambda_p \in \mathbb{C}$ such that $L_{A_6A_2}L_{A_5A_3}L_{A_1A_4} + \lambda_p LA_1A_5L_{A_2A_4}L_{A_3A_6}$ [Take $\lambda_p = \frac{-L_{A_4A_2}(P)L_{\ldots}(P)L_{\ldots}(P)}{L(\ldots)L(\ldots)L(\ldots)}$]. But then $L_{A_6A_2}L_{A_5A_3}L_{A_1A_4} + \lambda_p LA_1A_5L_{A_2A_4}L_{A_3A_6} = CL$ (TODO) □

2 Algebraic Geometry

For $\mathbb{A}^n$, $R = F[x_1, \ldots, x_n]$, and an ideal $I \subset R$ we have a **vanishing ideal** $V(I) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for any } f \in I\}$. For finitely generated $I = (f_1, \ldots, f_n) = \{g_1 f_1 + \cdots + g_n f_n\}$, we have $V(I)$ is the set of solutions of $\{f_i(x_1, \ldots, x_n) = 0\}$. We will prove soon that all ideals of $F[x_1, \ldots, x_n]$ are finitely generated. People name $V(I)$ **affine sets**, affine algebraic sets, affine algebraic varieties, or affine closed sets.

Some properties:

1. $V((1)) = \emptyset$.
2. $V((0)) = \mathbb{A}^n_{\mathbf{F}}$.
3. $V(I_1 \cup I_2) = V(I_1) \cap V(I_2)$ (inclusion $\supset$ is obvious. For $p \in V(I_1 \cup I_2)$, if $p \notin V(I_1)$, $f \in I_1$, so $f(p) \neq 0$, same with I_2, so $fg \in I_1 \cap I_2$...)
4. $\cup V(I_\alpha) = V(\prod I_\alpha)$, where $\prod I_\alpha$ is the ideal generated by polynomials $f_1 f_2 \ldots$ where $f_1 \in I_1, f_2 \in I_2, \ldots$.

These properties imply that affine sets are closed sets of a topology, called the **Zariski topology**.

"I have 20 more minutes? *Claps hands*"

Example 8. *1. If $\mathbb{A}^1_{\mathbb{C}}$, $R = \mathbb{C}[x]$, thus affine algebraic sets are either finite collections of points or $\mathbb{A}^1$.*

2. In $\mathbb{A}^2_{\mathbb{C}}$ we have a more complicated picture, we could have finite collections of points + quadrics and lines.

Definition 12. *Suppose R is a ring (commutative with 1). R is **Noetherian** if (TFAE)*

1. *Every ideal $I \subset R$ is finitely generated.*
2. *Every ascending chain $I_1 \subset I_2 \subset I_3 \subset \cdots \subset R$ stabilizes, so for some N, $I_N = I_{N+1} = I_{N+2} = \ldots$.*

Equivalence of these two conditions is on HW3. Geometrically, the Noetherian condition will tell us that infinite systems don't give us any new options for affine sets.

Example 9. *1. A field $\mathbf{F}$, every ideal is generated by 0 or 1.*

2. $\mathbb{Z}$, $\mathbf{F}[x]$, generated by $a \in \mathbb{Z}$ and x^n respectively.

3. If R is Noetherian, R/I is Noetherian.

4. Hilbert basis theorem: If R is Noetherian, $R[x]$ is Noetherian.

5. $F[x_1, \ldots, x_n]$ is Noetherian.

6. By the above $F[x_1, \ldots, x_n]/I$ is Noetherian. In particular, we will study $\mathbb{C}[x, y]/(x^2 + y^2 + 1)$, vanishing functions on a circle.

(Akhil Spectral theory notes are very good)

Theorem 13 (Hilbert Basis Theorem)**.** *R Noetherian if and only if $R[x]$ is Noetherian.*

Proof. Say $I \subset R[x]$ is an ideal, and let f_1 be an element in I of the smallest degree, f_2 be the element of smallest degree in $I \backslash (f_1)$, f_3 smallest degree in $I \backslash (f_1, f_2)$, ... Then we get a chain of distinct ideals $(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \dots$. Let's look at the leading coefficients a_i of f_i. Then, $(a_1, \dots,) = (a_1, \dots, a_n)$ is finitely generated. Thus, $a_{n+1} \in (a_1, \dots, a_n)$, and as such $a_{n+1} = a_1\lambda_1 + \dots + a_n\lambda_n$. Suppose we have $f_{n+1} \in (f_1, \dots, f_n)$. Then, let

$$g = f_{n+1} - \lambda_1 f_1 x^{\deg f_{n+1} - \deg f_1} - \dots - \lambda_n f_n x^{\deg f_{n+1} - \deg f_n}$$

so $\deg g < \deg f_{n+1}$, but $g \in I \setminus (f_1, \dots, f_n)$, which contradicts the choice of f_{n+1}. □

2.1 Lecture 8

There exists a correspondence between affine algebraic sets in $\mathbb{A}^n$ and the ideals on $k[x_1, \dots, x_n]$. Indeed, we can take any ideal I on $k[x_1, \dots, x_n]$ and consider its vanishing set $V(I)$. Note the following properties we reviewed last time: $V(I \cap J) = V(I) \cup V(J)$ and $I \subset J \implies V(I) \supset V(J)$. This correspondence can be reversed: take some affine algebraic X and consider $I(X) = \{f \in k[x_1, \dots, x_n] \mid \forall p \in X, f(p) = 0\}$. So given X, relate to it the ideal of functions that vanish on it.

Note that this correspondence is not invertible: consider $I \subset \mathbb{R}[x, y]$ generated by $x^2 + y^2 + 1 = 0$. The vanishing set of this is empty, but $I(\emptyset) = \mathbb{R}[x, y]$. Also could consider $k = \mathbb{C}$ and first consider $I = (x^2)$. However

Proposition 2. *For any affine algebraic set $X \subset \mathbb{A}^n$ we have $V(I(X)) = X$. So, $X \to I(X)$ is an injective map.*

Proof. Set $X = V(f_1, \dots, f_n)$, solutions to the system of f_i. If $p \in X$, then $p \in V(I(X))$. On the other hand if $p \in V(I(X))$, every f which vanishes on X vanishes on p. Thus, all f_i vanish on p so $p \in X$. □

Definition 13. *Let $I \subset R$ be an ideal in a ring. The **radical** of I, denoted $\sqrt{I}$, is given by $\{z \in \mathbb{R} \mid \exists N\ z^N \in I\}$.*

This is an ideal (homework). An example of how this works is $\sqrt{(x^2)} = (x)$.

Definition 14. *I is **radical** if $\sqrt{I} = I$.*

Theorem 14 (Hilbert's Nullstellensatz)**.** *For an ideal $J \subset k[x_1, \dots, x_n]$ (k is algebraically closed), we have $I(V(J)) = \sqrt{J}$.*

Example: $(x^2) \xrightarrow{V} 0 \in \mathbb{A}^1 \xrightarrow{I} (x) = \sqrt{(x^2)}$.

'Middle school version': consider $f_1, \dots, f_m \in \mathbb{C}[x_1, \dots, x_n]$. Suppose that $g \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every solution of the system $\{f_i = 0\}_i$. Then there exists some natural N such that $g^N \in (f_1, \dots, f_n)$, an ideal of $\mathbb{C}[x_1, \dots, x_n]$.

Definition 15. *An affine algebraic set X is called **irreducible** if it cannot be presented as a union of affine algebraic sets. Thus, if $X = X_1 \cap X_2$ is irreducible, X_1 or X_2 is X.*

Theorem 15. *X is irreducible iff $I(X)$ is prime (recall: I prime if $ab \in I$ then either a or b in I).*

Proof. Suppose $I(X)$ is not prime, so there exist $f, g \in k[x_1, \ldots, x_n]$ so $fg \in I(X)$ but $f, g \notin I(X)$. Take $X_1 = X \cap V(f)$, $X_2 = X \cap V(g)$ ($V(f)$ is the vanishing set). Then $X = X_1 \cup X_2$, but $X_1, X_2 \neq X$.

Suppose X is not irreducible, so $X = X_1 \cup X_2$ with $X_1, X_2 \neq X$. So $I(X) \neq I(X_1)$, in fact $I(X) \subset I(X_1)$, similarly $I(X) \subset I(X_2)$ (subsets strict). As such, there exist $f \in I(X_1)$, $g \in I(X_2)$, thus fg vanishes on $X_1 \cup X_2$, so $fg \in I$, and I is not prime. □

Theorem 16. *Suppose $X \subset \mathbb{A}^n$ is an affine algebraic set. Then*

1. *There exist irreducible affine sets $X_1, \ldots, X_m$ such that $X = X_1 \cup \cdots \cup X_m$, and $X_i \supset X_j$ (strict).*
2. *This decomposition is unique up to relabeling the sets X_i.*

Proof. If X is irreducible, we are done. Otherwise, $X = X_1 \cup X_2$, a union of proper subsets. Continue recursively until we obtain a binary tree of affine sets, where the leaves (terminating nodes) are irreducible. Suppose for contradiction the tree we obtain this way is infinite, then there exists an infinite path down the tree: $X \supset X^{(1)} \supset X^{(2)} \supset \ldots$. Then $I(X) \subset I(X^{(1)}) \subset I(X^{(2)}) \subset \ldots$. But this contradicts the fact that X is Noetherian.

Suppose we have two decompositions $X_1 \cup \cdots \cup X_m = X_1' \cup \ldots X_m'$. Take any X_i, then $X_i = X \cap X_i = (X_1' \cap X_i) \cup (X_2' \cap X_i) \cdots \cup (X_m' \cap X_i)$. Because X_i is irreducible, this implies $X_i = X_i \cap X_j'$, and as such $X_i \subset X_j'$. But performing this same argument for X_j' we get $X_i \subset X_j' \subset X_k$, so $X_i = X_k$, and $X_i = X_j'$. □

Main example of affine sets are hypersurfaces: if $f(x_1, \ldots, x_n)$ is an irreducible polynomial of non-zero degree, its vanishing set is an irreducible **hypersurface**. An example would be something like $xyz \pm x^2 + y^2 + z^2 + 1 = 0$.

Recall our correspondence between algebraic sets and ideals of $k[x_1, \ldots, x_n]$ from the beginning. Note that by Nullstellensatz $I(X)$ for any affine algebraic set X is a radical ideal. So, restricting our correspondence to radical ideals, is correspondence becomes bijective. This same correspondence carries irreducible sets to prime ideals, hypersurfaces to principal ideals, and maximal ideals to points.

Now we need some notions from commutative algebra.

Suppose A and B are algebras over the same field k. Assume $A - B$, so $A \supset B$ as sets. Say that A is **finitely generated over** B if there exist $a_1, \ldots, a_n \in A$ such that $A = B[a_1, \ldots, a_n]$: every $a \in A$ is a polynomial in $a_1, \ldots, a_n$ with coefficients in B. Example: $k[x_1, \ldots, x_n]$ finitely generated algebra over k. Another one is $\mathbb{C}[x, y]/(x^2+y^2-1)$ is a finitely generated algebra over $\mathbb{C}$.

We say A is **finite** over B [if A is a finitely generated B-module] if there exist $a_1, \ldots, a_n \in A$ such that for all $a \in A$ there are $b_1, \ldots, b_n \in B$ so $a = a_1 b_1 + \ldots a_n b_n$. In other words, $A = a_1 B + a_2 B + \cdots + a_n B$. Example: $\mathbb{C}[x]/(x^3 - 1)$, this is a finite algebra over $\mathbb{C}$, in fact a three-dimensional vector space. If your algebra is also a field, another algebra being finite over it means you have a finite-dimensional vector space.

2.2 Lecture 9

Definition 16. *A if **finitely generated over** B if there exist $a_1, \ldots, a_n \in A$ such that every element in A is a polynomial in a_i with B-coefficients: $A = B[a_1, \ldots, a_n]$. In other words, $B[x_1, \ldots, x_n] \to A$ with the map being the evaluation homomorphism $f \mapsto f(a_1, \ldots, a_n)$ is surjective. In other words, $A \cong B[x_1, \ldots, x_n]/I$.*

Another definition, A is finite over B [A is finite as a B-module] if there exist $a_1, \ldots, a_n$ if for every $a \in A$ there exist $b_1, \ldots, b_n$ such that $a = b_1a_1 + \cdots + b_na_n$.

Here's a key bit from commutative algebra:

Theorem 17. *Let k be a field of characteristic 0. Suppose that A is a finitely generated algebra over k, so $A = k[x_1, \ldots, x_n]/I$. Assume A is a field. Then A is a finite algebraic extension of k.*

(Choosing $k = \mathbb{C}$, we know that every finitely generated algebra over $\mathbb{C}$ that's a field must be $\mathbb{C}$ itself.)

We now want to show that in the correspondence we talked about last lecture, finite sets of points correspond to maximal ideals of $k[x_1, \ldots, x_n]$.

Take $P = (a_1, \ldots, a_n) \subset \mathbb{A}^n$ be a set of points in $\mathbb{A}^n$. Consider that the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ generated by these n linear elements is then a subset of $I(P)$. Take any $f \in I(P)$, then $f(a_1, \ldots, a_n) = 0$ implies $f(a_1 + y_1, \ldots, a_n + y_n) = y_1f_1 + \cdots + y_nf_n$ for some functions $f_i \in I(P)$. THen $f(x_1, \ldots, x_n) - (x_1 - a_1)f_1 + \ldots (x_n - a_n)f_n$ which implies $f \in (x_1 - a_1, \ldots, x_n - a_n)$.

We further claim $I(P) = (x_1 - a_1, \ldots, x_n - a_n)$ is maximal. Consider the surjective map $k[x_1, \ldots, k_n] \to k$ given by the evaluation homomorphism $f \mapsto f(a_1, \ldots, a_n)$. Its kernel is $I(P)$. Then $k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k$, which implies $I(P)$ is maximal.

Now, for every maximal ideal $M \subset k[x_1, \ldots, x_n]$ there exist $a_1, \ldots, a_n$ such that $M = (x_1 - a_1, \ldots, x_n - a_n)$. Indeed, consider $k[x_1, \ldots, x_n]/M$, a finitely generated algebra over k, so by theorem it is finitely generated over k. Then, looking at the map $k \to k[x_1, \ldots, x_n]/M$, we know there are $a_1, \ldots, a_n$ such that k maps a_i and x_i to the same coset. Hence, $x_i - a_i \in M$, and $(x_1 - a_1, \ldots, x_n - a_n) \subset M$. Because both sides are maximal ideals, this in fact implies equality. This proves the correspondence between points and maximal ideals.

Now we show weak Nullstellensatz: the empty set corresponds to all of $k[x_1, \ldots, x_n]$. Suppose the system of $f_1, \ldots, f_m \in k[x_1, \ldots, x_m]$ has no solutions, i.e. there exist $u_1, \ldots, u_m$ such that $1 = f_1u_1 + \ldots f_mu_m$. Indeed, suppose not, then there exists a maximal ideal M with $(f_1, \ldots, f_m) \subset M$, then there exist a_i such that $x_i - a_i$ generate it. So $(f_1, \ldots, f_m) \subset (x_1 - a_1, \ldots, x_n - a_n)$, hence $(a_1, \ldots, a_m)$ is a solution to this system, contradiction.

Now show strong Nullstellensatz. Suppose that $g \in k[x_1, \ldots, x_n]$ vanishes at every point p that's a solution to $\{f_i(p) = 0\}$ (this system has solutions). Then there exists N such that $g^N \in (f_1, \ldots, f_m)$. Consider $k[x_1, \ldots, x_n] \subset k[x_1, \ldots, x_n, t]$. Consider an ideal $J = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_m), tg(x_1, \ldots, x_m) - 1)$, we know $V(J) = \emptyset$. Then there exist some polynomials $u_1, \ldots, u_{m+1} \in k[x_1, \ldots, x_m, t]$ such that $u_1f_1 + \cdots + u_mf_m + u_{m+1}(tg - 1) = 1$. Plug in $t = \frac{1}{g}$, then $u_1(x_1, \ldots, x_n, 1/g)f_1(x_1, \ldots, x_n) + \cdots = 1$, and

$$\frac{\tilde{u}(x_1, \ldots, x_n)}{g^m} f_1(x_1, \ldots, x_m) + \cdots + \frac{\tilde{u}(x_1, \ldots, x_m)}{g^m} = 1$$

Multiply by g^m on both sides and we are done. This type of reduction of strong to weak Nullstellensatz is called the Rabinovich trick.

Now we should probably prove the commutative algebra result we've been relying on.

Lemma 2. *If $A - B$ and $B - C$ are finite then $A - C$ is finite.*

Proof. Express $A = a_1B + a_2B + \dots a_nB$, $B = b_1C + \dots b_mC$, plug in the latter into the former. □

Lemma 3. *Suppose $A - B$ finite, then for $a \in A$ there exist $n \in \mathbb{N}$, $b_0, \dots, b_{n-1} \in B$ then $a^n + b_{n-1}a^{n-1} + \dots + b_0 = 0$ [a is integral over B].*

Proof. A is finite over B, thus there exist $a_1, \dots, a_n$ such that $A = Ba_1 + \dots + Ba_n$, so

$$\begin{cases} aa_1 = b_{11}a_1 + \dots + b_{1n}a_n \\ aa_2 = b_{21}a_1 + \dots + b_{2n}a_n \\ \vdots aa_n = b_{n1}a_1 + \dots + b_{nn}a_n \end{cases}$$

Subtracting aa_i from the left we get a system, and from it we get

$$\det \begin{bmatrix} b_{11} - a & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} - a & \dots & b_{2n} \\ \vdots b_{n1} & b_{n2} & \dots & b_{nn} - a \end{bmatrix} = 0$$

There exists an *adjunct* matrix X^* to the matrix X above such that $X^*X = \det X \mathrm{Id} X*$. Then we also get $(\det X)a_i = 0$ and $\det X = b_1a_1 + \dots$ (TODO) □

Final lemma: $B[x] - B$ is finite.