Algebraic Geometry Notes

Raman Aliakseyeu

Winter 2024

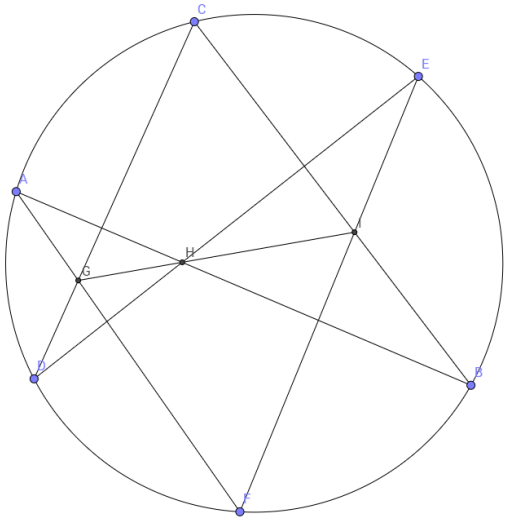
Course by Daniil Rudenko.

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 1.1. *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 1.2. *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 1.3. *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 1.1. *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.

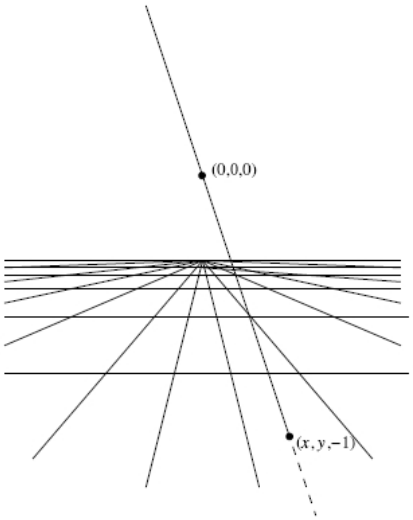
In $\mathbb{R}^2$, usually two lines intersect at one point, and two points are contained in one line. We can also define $\mathbb{P}^2_{\mathbb{R}}$ as the set of points of $\mathbb{R}^2$, and the set $[l]$ (points at ∞), which are equivalence classes of lines in $\mathbb{R}^2$ by $l_1 \sim l_2$ for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

Fact 1.4. *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 1.5. *For $\mathbb{P}^2_{\mathbb{R}}$, the abstract definition 1.1 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. • *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 1.2. *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. *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 1.3. *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.
- *$P_1(x, y) = 2x + y - 1 = 0$ 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 1.4. *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 1.1. *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 1.2. *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 1.5. *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 $\mathbb{A}^n$. The points with $X_n = 0$ are in bijection with points in $\mathbb{A}^{n-1}$ (divide all entrees by the first non-zero entry from the right). Indeed, $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0$. 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, M 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 1.6. ***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. *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 $f : V_1 \to V_2$ between vector spaces V_1 and 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 1.7. *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 $\mathrm{PGL}(V) = \mathrm{PGL}_n(\mathbf{F})$.*

$\mathrm{PGL}_n(\mathbf{F})$ 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 $\ker \Phi$ consists of all multiples of the identity, which is isomorphic to $\mathbf{F}^\times$. So, $\mathrm{PGL}_n(\mathbf{F}) = \mathrm{GL}_n/\mathbf{F}^\times$ by first isomorphism theorem.

Now consider $\mathbb{P}^1_{\mathbf{F}}$, and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbf{F})$. Then $f([x : y]) = [ax + by : cx + dy]$. The fact the matrix is in GL gives $\det = ad - bc \neq 0$. Note that we can interpret $\mathbb{P}^1_{\mathbf{F}} = \mathbb{A}^1_{\mathbf{F}} \cup \infty$, where $\mathbb{A}^1_{\mathbf{F}}$ can be thought of as the set of all $[x : 1]$, and ∞ can be thought of as $[1 : 0]$. So on $\mathbb{A}^1_{\mathbf{F}}$, $f([x : 1]) = [ax + by : cx + dy] = [\frac{ax+b}{cx+d} : 1]$. This implies that on the affine line $\overline{f}$ sends x to $\frac{ax+b}{cx+d}$.

Example. *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 our 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.

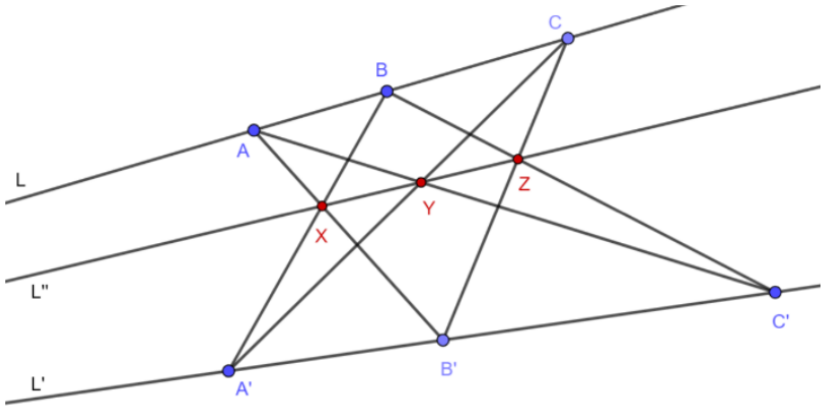
Theorem 1.3. *Consider points $A_1, \dots A_{n+2}$, $B_1, \dots, B_{n+2}$ in $\mathbb{P}^n$ such that $\{A_i\}$ and $\{B_i\}$ are in general position (on $\mathbb{P}^n$ this means for any i, $A_1, \dots, \hat{A}_i, \dots, A_{n+2}$ span $\mathbf{F}^{n+1}$ when considered as vectors in $\mathbf{F}^{n+1}$). Then there exists a unique $\overline{f} \in \mathrm{PGL}_n(\mathbf{F})$ such that $\overline{f}(A_j) = B_j$ for $1 \leq j \leq n + 2$.*

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 $v_1, \dots, v_{n+1}$ and $w_1, \dots, w_{n+1}$ are bases of $\mathbf{F}^{n+1}$, so there exists a unique invertible linear transformation f_1 such that $f_1(v_i) = w_i$. Since $v_{n+2} = \lambda_1 v_1 + \dots + \lambda_{n+1} v_{n+1}$, we know

$f(v_{n+2}) = \lambda_1 w_1 + \ldots \lambda_{n+1} w_{n+1}$. Consider now $w_{n+2} = \mu_1 w_1 + \cdots + \mu_{n+1} w_{n+1}$. Note that this means $\lambda_i \neq 0$ for any i since otherwise there exists a subset $v_1, \ldots, \hat{v_i}, \ldots, v_{n+2}$ that does not span $\mathbf{F}^{n+1}$. Similarly, $\mu_i \neq 0$. 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 $f_2 \circ f_1(v_{n+2}) = w_{n+2}$. Note that this map is also invertible. As such, there exists a projective transformation $\overline{f_2 f_1}$ which sends A_i to B_i.

Uniqueness (ASK ABOUT) □

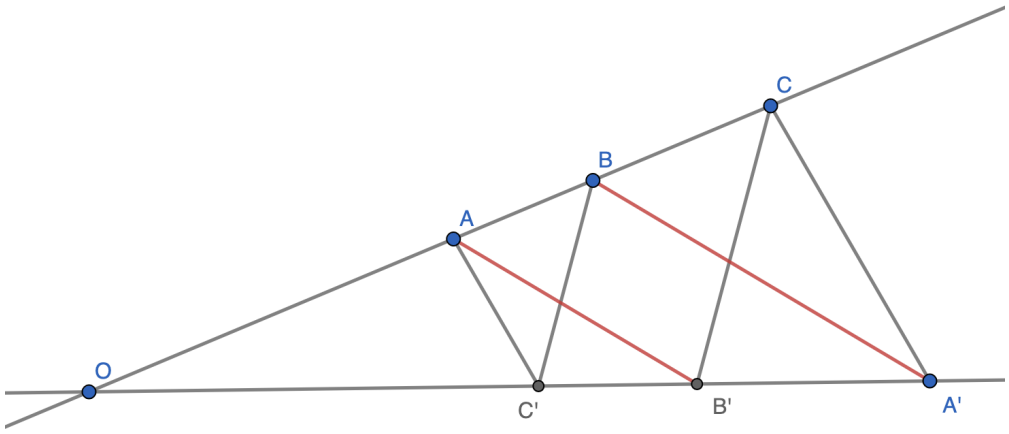
Theorem 1.4 (Pappus' Theorem)**.** *Consider the diagram*



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 $\overline{A'B}$.

Suppose after the transformation the lines intersect at point O.



Because AC' and $A'C$ are parallel, as well as BC' and $B'C$, we have that $\triangle AOC'$ and $\triangle COA'$ are similar, same with $\triangle BOC'$ and $\triangle COB'$. From this we obtain the relations

$$\frac{|OA|}{|OC'|} = \frac{|OC|}{|OA'|} \quad \frac{|OB|}{|OC'|} = \frac{|OC|}{|OB'|}$$

Then,

$$\frac{|OA|}{|OB|} = \frac{|OA|}{|OC'|}\frac{|OC'|}{|OB|} = \frac{|OC|}{|OA'|}\frac{|OB'|}{|OC|} = \frac{|OB'|}{|OA'|}$$

Because they share an angle and because a pair of their corresponding sides has the same ratio, triangles $\triangle AOB'$ and $\triangle BOA'$ must be similar. By the parallel line postulate we are done. □

For $\mathbb{P}^1$, recall that $\mathrm{PGL}_2(\mathbf{F}) = \left\{\frac{ax+b}{cx+d} \mid ad - bc \neq 0\right\}$. 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 1.8. *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 1.5. *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. Note that $\mathrm{PGL}_2(\mathbf{F})$ as a group is generated by the elementary matrices (considered as being projective transformations) of the form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The first matrix acts on $x \in \mathbb{P}^1_{\mathbf{F}}$ by multiplying it by a/d. This of course does not change the cross ratio. The second matrix maps $x \mapsto x + b$, which also doesn't change the cross ratio, since b's cancel in each pair of parentheses in the expression for the cross ratio. The last matrix maps $x \mapsto 1/x$. In this case, if $x_i < \infty$,

$$\frac{\left(\frac{1}{x_1} - \frac{1}{x_2}\right)\left(\frac{1}{x_3} - \frac{1}{x_4}\right)}{\left(\frac{1}{x_1} - \frac{1}{x_4}\right)\left(\frac{1}{x_3} - \frac{1}{x_2}\right)} = \frac{(x_2 - x_1)(x_4 - x_3)}{(x_4 - x_1)(x_2 - x_3)}$$

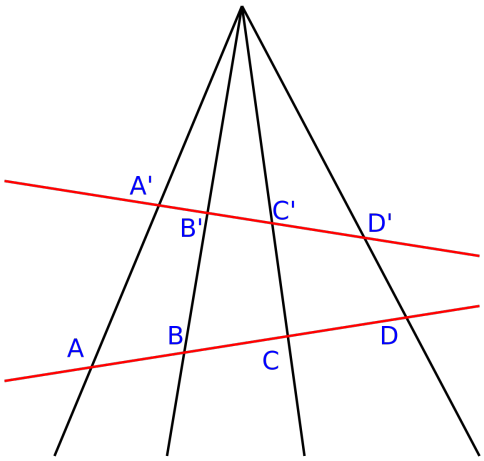
Which is the same as the original cross-ratio. If say $x_4 = \infty$ we have

$$\frac{\left(\frac{1}{x_1} - \frac{1}{x_2}\right)\left(\frac{1}{x_3} - \frac{1}{x_4}\right)}{\left(\frac{1}{x_1} - \frac{1}{x_4}\right)\left(\frac{1}{x_3} - \frac{1}{x_2}\right)} = \frac{\left(\frac{1}{x_1} - \frac{1}{x_2}\right)\frac{1}{x_3}}{\left(\frac{1}{x_1}\right)\left(\frac{1}{x_3} - \frac{1}{x_2}\right)} = \frac{x_2 - x_1}{x_2 - x_3}$$

which is again the same as the original cross ratio. Since all the generators of $\mathrm{PGL}_2(\mathbf{F})$ preserve the cross ratio, so must all its elements. □

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 1.1. *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 $\mathbb{P}^1 \to \mathbb{P}^1$. As a map between planes, this takes a point on $p \in L_i$ to its perpendicular projection onto $V/O \neq L_i$. This map is a bijective homomorphism, so its invertible. Indeed, we have the commutative diagram

$$\begin{array}{ccccc} & V & & V & \\ \nearrow & & \searrow \quad \swarrow & & \nwarrow \\ L_1 = \mathbb{P}^1 & & \longrightarrow V/O = \mathbb{P}^1 \longleftarrow & & L_2 = \mathbb{P}^1 \end{array}$$

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

In particular, this implies that a projective transformation on $\mathbb{P}^2$ preserves cross ratio.

1.4 Lecture 4

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 $V = \mathbf{F}^n$ ($\{x_i\}$ is precisely the basis of V^* dual to the standard basis $\{e_i\}$ of V). $R_2 = \mathbb{S}^2 V^*$, and in general $R_d = \mathbb{S}^d V^*$.

Definition 1.9. *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. *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) is $(x_0/x_3)^3 - (x_1/x_3)^3 + x_2/x_3 + 1 = 0$. The rest of this hypersurface is in $\mathbb{P}^3 \setminus \mathbb{A}^3 = H$, in this H, the hypersurface 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 1.10. *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 1.11. *A hypersurface $X = \{F = 0\}$ for $F \in R_d$ is **irreducible** precisely when F is irreducible.*

Example.

- *$x_0 x_1 = 0$ 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 is 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 $d = 2$, polynomial F looks like

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

With a symmetric matrix A. Subject to a projective transformation, $x = Uy$ for some $y \in \mathbb{P}^2$, $U \in \mathrm{PGL}_{n+1}$. Thus, $x^\top A x = 0 \mapsto (Uy)^\top A (Uy) = y^\top (U^\top A U) y^\top 0$. Note that because A is symmetric, it is diagonalizable, hence for some U, $U^\top A U$ is a diagonal matrix of eigenvalues of A. In this case, we have shown:

Theorem 1.6. *Any quadric is a projectively equivalent to a quadric $\lambda_0 x_0^2 + \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 = 0$ (with some λ_i possibly zero).*

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 $x_0^2 + x_1^2 + \cdots + x_i^2 = 0$ (from the theorem above by applying a shearing transformation). 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.

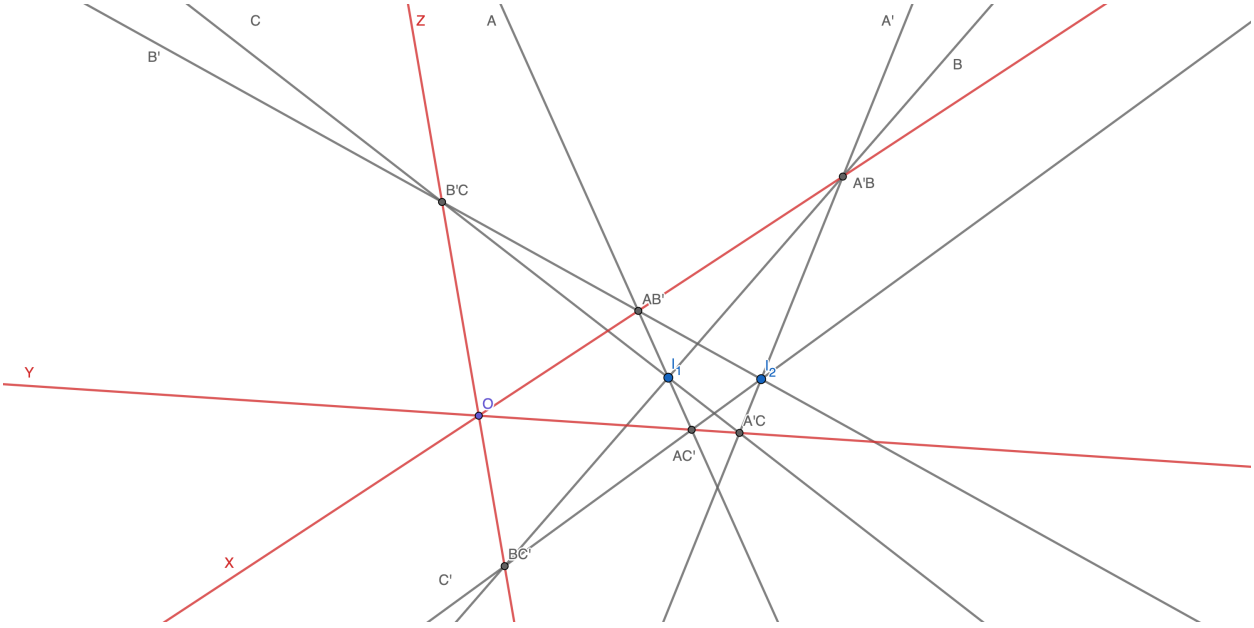
Now we discuss projective duality. Suppose we are working in $\mathbb{P}^2$. A line here is defined by an equation $ax + by + cz = 0$ with not all $a, b, c = 0$, modulo rescaling. Thus lines in $\mathbb{P}^2$ also form a projective space. This has some striking applications.

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. *Recall Pappus' theorem. We can state it as follows: Consider lines l_1, l_2 and points A, B, C on l_1 and A', B', C' on l_2. Let X be the intersection of lines AB' and $A'B$, Y the intersection of AC' and $A'C$, and Z the intersection of BC' and $B'C$. Then X, Y, Z are colinear.*

The dual is: Given points l_1, l_2 and lines A, B, C through l_1 and A', B', C' through l_2, let X be the line through points AB' and $A'B$, intersections of lines $A \cap B'$ and $A' \cap B$ respectively. Define Y, Z similarly. Then lines X, Y, Z intersect in some point O. Diagram below:



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

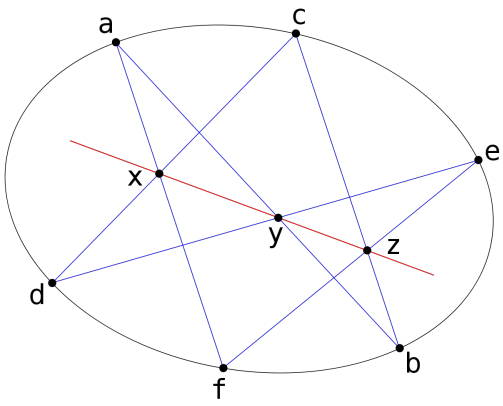
Three important facts about V^*: 1. $\dim V = \dim V^*$ since V and V^* are (not canonically) isomorphic, 2. $V \cong (V^*)^*$ canonically via an isomorphism $v \mapsto (\varphi : V \to F \mapsto \varphi(v))$, 3. There is an inclusion reversing bijection between subspaces of V and V^*, which is equivalent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

1.5 Lecture 5

Let's talk about conics a little bit more. If $\mathbb{P}^n_{\mathbf{F}} = \mathbb{P}(\mathbf{F}^{n+1})$, $[x_0 : x_1 : \cdots : x_n]$ are homogeneous coordinates on $\mathbb{P}^n_{\mathbf{F}}$, and $P(x_0, \ldots, x_n)$ is a homogeneous polynomial of degree d, we have that $\{[x_0, \ldots, x_n] \mid P(x_0, \ldots, x_{n+1}) = 0\} \subset \mathbb{P}^n$ 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). A conic is called the *smooth* quadric.

Theorem 1.7 (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 $\mathbb{C}$.

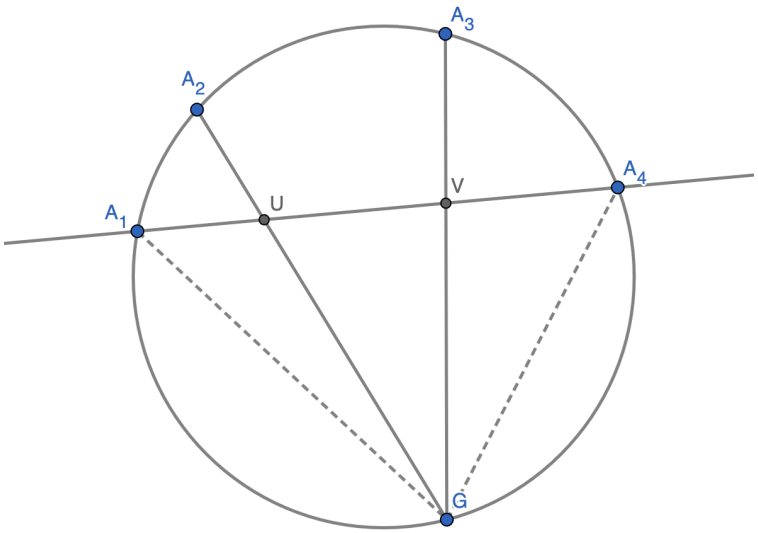
Lemma 1.1 (Chasles)**.** *Let points A_1, A_2, A_3, A_4 and X, Y lie on a conic. Then*

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

(Identification of a conic with $\mathbb{P}^1$ is explained below).

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 with infinity 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. Without loss of generality 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. (see diagram below)



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 (we get the second equality since the altitude to X is the same). Since they are inscribed angles, 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). (TODO: relabel points either on diagram or here) 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* to the product up to

multiplicity. The hard part about the equality is that 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 1.8 (Sylvester)**.** *Let $A(x)=a_mx^m+a_{m-1}x^{m-1}+\dots a_0=0$ 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*

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

(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 1.9. *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*

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

Proof. Let's view $\mathrm{Res}(f,g)$ 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 $\mathrm{Res}=a_m^nb_n^mP(t_1,\dots,t_m,s_1,\dots,s_n)$.

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 $\tilde{f}(x)=f(x+x_0)=\tilde{a}_nx^n+\dots+\tilde{a}_0$. But

then $f(x) = \tilde{a}_n(x - x_0)^n + \cdots + \tilde{a}_0$, 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 $\mathbb{Z}[t_1, \ldots, \hat{t}_i, \ldots, t_m, s_1, \ldots]$. Thus, $P(s_j) = 0$ implies $(t_i - s_j) \mid P$. Note that $(t_i - s_j)$ are pairwise coprime, as such

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

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 1.10 (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. □

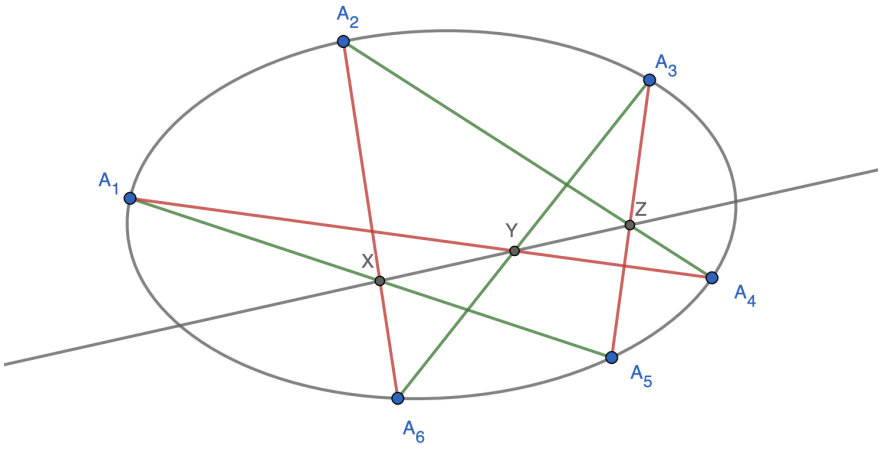
1.7 Lecture 7

Theorem 1.11. *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 conic containing $P_1, \ldots, P_5$.*

Proof. Consider $\mathbb{P}^5 = \mathbb{P}(\mathbb{S}^2 V^*)$, the space of quadrics $F = ax^2 + by^2 + cz^2 + dxy + exz + yz$ in $\mathbb{P}^2$, corresponding to the coordinate $[a : b : c : d : e : 1]$. For a $P \in \mathbb{P}^2$, the set H_{P_i} of quadrics containing $P_i = [x_i : y_i : 1]$ forms a 4-hyperplane in $\mathbb{P}^5$, the intersection of $\mathbb{P}^5$ with a 5-hyperplane in $\mathbb{C}^6$ corresponding to the set $ax_0^2 + by_0^2 + cz_0^2 + dx_0y_0 + ex_0z_0 + y_0z_0 = 0$. Because $P_i = [x_i : y_i : z_i] = [x_i/z_i : y_i/z_i : 1]$ are in general position, then so are vectors $[x_i^2, y_i^2, z_i^2, x_iy_i, x_iz_i, y_iz_i] = [(x_i/z_i)^2, (y_i/z_i)^2, 1, x_iy_i/z_i^2, x_i/z_i, y_i/z_i]$ (look at the last two coordinates). Hence, the 5 hyperplanes corresponding to H_{P_i} in $\mathbb{C}^6$ are in general position also, so they must intersect at precisely one point. Thus, P_i specify a unique quadric. Because P_i are in general position, we cannot have the quadric be a line or a union of two lines, because then one of the lines would have to contain three of the points. Hence, the quadric containing these points is indeed a conic. □

Using this we can prove Pascal's theorem in a different way:

Theorem 1.12 (Pascal's theorem on conic)**.** *Take $C = 0$ defining an irreducible conic, $A_1, \ldots, A_6$, $X = A_1A_5 \cap A_2A_6$, ... Then X, Y, Z lie on the same line.*



Proof. Denote by L_{UV} be the equation for the line through some points U, V. Consider cubic curves $R = L_{A_6A_2}L_{A_5A_3}L_{A_1A_4}$ (in red) and $G = L_{A_1A_5}L_{A_2A_4}L_{A_3A_6}$ (in green). These intersect at $A_1, \ldots, A_6, X, Y, Z$. Consider any point $P \in C$ that is not $A_1, \ldots, A_6$. Then there exists $\lambda_p \in \mathbb{C}$ such that $(R + \lambda_p G)(P) = 0$ [Take $\lambda_p = \frac{-R(P)}{G(P)}$]. Then $R + \lambda_p G = 0$ is degree 3 curve that has 7 points in common with the quadric C. But by weak Bezout's, C and $R + \lambda_p G$ can intersect in at most 6 unless they have a component in common. Since C is irreducible, their common component must be C itself, hence $R + \lambda_p G$ must be a union of C and a line. The three points X, Y, Z that do not lie on C must then lie on a line. □

2 Algebraic Geometry

For $\mathbb{A}^n$, $R = k[x_1, \ldots, x_n]$, 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 that $V(I)$ is the set of solutions of $\{f_i(x_1, \ldots, x_n) = 0\}$. We will prove soon that all ideals of $k[x_1, \ldots, x_n]$ are finitely generated. People call $V(I)$ **affine sets**, affine algebraic sets, affine algebraic varieties, or affine closed sets.

Some properties:

1. $V((1)) = \emptyset$.
2. $V((0)) = \mathbb{A}^n_k$.
3. For ideals $I, J \subset k[x_1, \ldots, x_n]$,

$$V(I) \cup V(J) = V(IJ)$$

where IJ is the ideal generated by products fg for $f \in I$, $g \in J$.

Proof. Inclusion $V(I) \cap V(J) \subset V(IJ)$ is obvious. For the other inclusion, if $p \notin V(I)$ then for any $f \in I$, $f(p) \neq 0$. Similarly $p \notin V(J)$ implies any $g \in V(J)$ doesn't vanish on p. So if $p \notin V(I) \cup V(J)$, $fg(p) \neq 0$ also, hence p cannot be in $V(IJ)$. □

4. For a collection of ideals $I_\alpha \subset k[x_1, \ldots, x_n]$,

$$\cap_\alpha V(I_\alpha) = V(\sum_\alpha I_\alpha)$$

where $\sum_\alpha I_\alpha$ is an ideal consisting of sums of elements in various I_α, i.e. one generated by the elements of $\cup I_\alpha$.

Proof. If $p \in \cap_\alpha V(I_\alpha)$, then polynomials in every I_α vanish on p, hence their sums vanish also. If $p \in V(\sum_\alpha I_\alpha)$, for any α any element of I_α vanishes on p, hence the other inclusion holds. □

These properties imply that affine sets are closed sets of a topology on $\mathbb{A}^n_{\mathbf{F}}$, called the **Zariski topology**.

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

Example. *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 2.1. *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. *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.

(Vakil Spectral theory notes are very good)

Theorem 2.1 (Hilbert Basis Theorem)**.** *R Noetherian if and only if $R[x]$ is Noetherian.*

Proof. One direction is simple: if I is an ideal of R, it is also an ideal of $R[x]$. If $R[x]$ is Noetherian, R is finitely generated as an ideal of $R[x]$, but since I is also an ideal of R, all its generators must be in R also. But then I is finitely generated over R also.

In the other direction, say $I \subset R[x]$ is an ideal, and let f_0 be an element in I of the smallest degree, f_1 be an element of smallest degree in $I-(f_0)$, f_2 smallest degree in $I-(f_0,f_1)$ ...(− is set subtraction). Suppose for contradiction that I is not finitely generated, so we can keep choosing f_i indefinitely. Consider the leading coefficients a_i of f_i, and the chain of ideals

$$(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \dots$$

This is an ascending chain of ideals in R, hence it must stabilize at some ideal $(a_0, \dots, a_{n-1})$. Thus, the ideal of leading coefficients of f_i must be generated by $a_1, \dots, a_{n-1}$. In particular, the leading coefficient a_n of f_n can be expressed like $\lambda_1 a_1 + \dots + \lambda_{n-1} a_{n-1}$. Then consider

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

(Note that by construction of our f_i, the exponents are valid) The leading term in the parentheses is the same as the leading term of f_n, so $\deg g < \deg f_n$. But also $g \in I - (f_1, \dots, f_{n-1})$ (since the term in the parantheses is in $(f_1, \dots, f_{n-1})$). This contradicts our choice of f_n earlier, so we are done. □

2.1 Lecture 8

There exists a correspondence between ideals on $k[x_1, \dots, x_n]$ and affine algebraic sets in $\mathbb{A}^n$. Indeed, we can take any ideal I on $k[x_1, \dots, x_n]$ and consider its vanishing set $V(I)$. In the other direction, 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, we can relate to it the ideal of functions that vanish on it. Note however 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 2.1. *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 $X = V(f_1, \dots, f_n)$, so X consists of points on which f_i vanish. If $p \in X$, then $p \in V(I(X))$ obviously. On the other hand if $p \in V(I(X))$, then all $f \in I(X)$ vanish on p. In particular, $f_1, \dots, f_n \in I(X)$ vanish on p, hence $p \in X$. □

Definition 2.2. *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 2.3. *I is **radical** if $\sqrt{I} = I$.*

Theorem 2.2 (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 $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$. Suppose that $g \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at every solution of the system $\{f_i = 0\}_i$. Then there exists some positive integer N such that g^N is in $(f_1, \ldots, f_n)$, an ideal of $\mathbb{C}[x_1, \ldots, x_n]$.

Definition 2.4. *An affine algebraic set X is called **irreducible** if it cannot be presented as a union of affine algebraic sets. Thus, if $X = X_1 \cup X_2$ is irreducible, X_1 or X_2 is X.*

Theorem 2.3. *X is irreducible iff $I(X)$ is prime.*

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

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 $f \in I(X_1) - I(X_2)$, $g \in I(X_2) - I(X_1)$, thus fg vanishes on $X_1 \cup X_2$, so $fg \in I(X)$ but neither $f, g \in I(X)$. □

Theorem 2.4. *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 $X_i \not\subset X_j$ for any $i \neq j$.*

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 algebraic subsets. Then decompose X_1, X_2, and 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: $X \supset X^{(1)} \supset X^{(2)} \supset \ldots$. which corresponds to an infinite chain of ideals $I(X) \subset I(X^{(1)}) \subset I(X^{(2)}) \subset \ldots$ with strict inclusions. But this contradicts the fact that X is Noetherian. So the tree must be finite, which must give us a finite decomposition of X into a union of irreducible sets X_i. To get the condition $X_i \not\subset X_j$, discard any set X_i which violates it.

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, we have $X_i = X_i \cap X_j'$ for some j, and as such $X_i \subset X_j'$. But performing this same argument for X_j' we get $X_j' \subset X_k$, so $X_i = X_k$, and indeed $X_i = X_j'$. □

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, the correspondence becomes bijective. This same correspondence carries irreducible sets to prime ideals, hypersurfaces to principal ideals (as we've shown in Theorem 2.3), and maximal ideals to single points (this is shown in the next lecture).

2.2 Lecture 9

Definition 2.5. *An algebra A over k is **finitely generated over** B (another k-algebra) (sometimes denoted by the tower $A-B$) 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. By the first isomorphism theorem, $A \cong B[x_1, \ldots, x_n]/I$.

Definition 2.6. *A is a **finite B-algebra** if there exist $a_1, \ldots, a_n$ if for every $a \in A$ there exist $b_1, \ldots, b_n$ such that $a = b_1a_1 + \cdots + b_na_n$. In other words, $A = Ba_1 + \cdots + Ba_n$.*

Here's a key bit from commutative algebra, to be proven later:

Theorem 2.5. *Let k be a field of characteristic 0. Suppose that A is a finitely generated over k. Assume A is a field. Then A is a finite k-algebra.*

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

Proposition 2.2. *For $P = \{a = (a_1, \ldots, a_n)\} \subset \mathbb{A}^n_k$, $I(P) \subset k[x_1, \ldots, x_n]$ is maximal. Conversely, if $M \subset k[x_1, \ldots, x_n]$ is maximal, then $V(M) \subset \mathbb{A}^n_k$ is a single point.*

Proof. Firstly, we show that $I(P)$ is precisely $(x_1 - a_1, \ldots, x_n - a_n)$. The ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is clearly a subset of $I(P)$. On the other hand, take any $f \in I(P)$, then $f(a_1, \ldots, a_n) = 0$, and $f(y_1 + a_1, \ldots, y_n + a_n)$ is some polynomial in y_i with coefficients in k. Plugging in $y = x_i - a_i$ we get that $f(x_1, \ldots, x_n)$ is a polynomial in $x_i - a_i$ with coefficients in k, i.e. $f \in (x_1 - a_1, \ldots, x_n - a_n)$. 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 by the first isomorphism theorem, $k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k$, a field, which implies $I(P)$ is maximal.

Conversely we show that 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 and a field, so by Theorem 2.5 it is generated by some $b_1, \ldots, b_n$ over k. Thus, the composition $\varphi : k \to k[x_1, \ldots, x_n] \xrightarrow{\pi} K = k[x_1, \ldots, x_n]/M$ is such that there exist $a_i \in k$ with $\varphi(a_i) = \pi(x_i)$. This implies that $(x_1 - a_1, \ldots, x_n - a_n) \subset m$, but $(x_1 - a_1, \ldots, x_n - a_n)$ as a maximal ideal, as proven above. Hence, $m = (x_1 - a_1, \ldots, x_n - a_n)$. □

Now we show

Proposition 2.3 (Weak Nullstellensatz)**.** *The vanishing set of $k[x_1, \ldots, x_n]$ is the empty set. In other words, if $J \subset k[x_1, \ldots, x_n]$ is a proper ideal, $V(J) \neq \emptyset$.*

Proof. Let $J = (f_1, \ldots, f_n) \subset k[x_1, \ldots, x_n]$, and suppose for the sake of contradiction that $V(J) = \emptyset$. Then there exists a maximal ideal $M = (x_1 - a_1, \ldots, x_n - a_n)$ for some a_i such that $(f_1, \ldots, f_m) \subset (x_1 - a_1, \ldots, x_n - a_n)$. But $V(M) = \{P\}$ is non-empty, and $V(M) \subset V(J)$. Contradiction. □

Now we prove Nullstellensatz.

Proof. We show that for any $f \in J = (f_1, \ldots, f_n)$, we have some N such that $f^N \in J$. Consider the ideal $J_f \subset k[x_1, \ldots, x_n, t]$ generated by $f_1, \ldots, f_n, ft - 1$. Then its vanishing ideal $V(J_f) = \{(P, b) \in \mathbb{A}_k^{n+1} \mid P \in J(F), bf(P) = 1\}$ is empty as the conditions are contradictory. Hence, $J_f = k[x_1, \ldots, x_n, t]$, in particular

$$1 = \left(\sum g_i f_i\right) + g_0(ft - 1)$$

Let N be the degree of the right hand side as a polynomial in t. Then, consider

$$f^N = \left(\sum G_i f_i\right) + G_0(ft - 1)$$

where G_i are polynomials in $x_1, \ldots, x_n, ft$ (by construction there should be enough f factors to associate each t factor with an f factor). Then, by passing this identity through the quotient by the ideal $(ft - 1)$ we get

$$f^N \equiv \sum h_i f_i$$

where $h_i(x_1, \ldots, x_n) = G_i(x_1, \ldots, x_n, 1)$. But the quotient map is injective, hence this identity holds in $k[x_1, \ldots, x_n]$. We conclude $f^N \in J$, so $I(V(J)) \subset \sqrt{J}$. Since the other inclusion is obvious, we are done. □

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

Lemma 2.1. *If $A - B$ and $B - C$ are finite then $A - C$ is finite.*

Proof. Express $A = a_1 B + a_2 B + \ldots a_n B$, $B = b_1 C + \ldots b_m C$, plug in the latter into the former. □

Lemma 2.2. *Suppose $A - B$ finite, then for $a \in A$ there exist $n \in \mathbb{N}$, $b_0, \ldots, b_{n-1} \in B$ then $a^n + b_{n-1}a^{n-1} + \cdots + b_0 = 0$ [a is integral over B].*

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

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

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

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

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 $\det X = b_1 a_1 + \ldots$ (TODO) □

Final lemma:

Lemma 2.3. *$B[x] - B$ is finite.*

2.3 Lecture 10

Now we should prove Theorem 2.5 from above, because everything relies on it. Let's restate it:

Theorem. *Let k be an infinite field, and A is a finitely generated algebra over k. Then A is a finite algebraic extension of k.*

We introduced three lemmas last time. Let's do a forth:

Lemma 2.4. *Let A be finite over B, If A is a field, then B is a field.*

Proof. Suppose $b \neq 0 \in B$. Then, $\frac{1}{b} \in A$, consider

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

multiplying both sides by b^n, and factoring, we get that $1/b$ is in B. □

Theorem 2.6 (Noether Normalization Theorem)**.** *Let A be a finitely generated algebra over k, so $A = k[a_1, \ldots, a_n]$. Then there exist $y_1, \ldots, y_m \in A$ such that 1. $y_1, \ldots, y_m$ are algebraically independent and 2. A is finite over $k[y_1, \ldots, y_m]$.*

Example. *Take $\mathbb{C}[x, y]/(y^2 - x^3y - 1)$. Consider that y is a root of a monic polynomial with coefficients in $\mathbb{C}[x]$ in this field, namely $y^2 - x^3y - 1 = 0$. Hence this field is finite over $\mathbb{C}[x]$. However, the same does not hold for x, so this field is not finite over $\mathbb{C}[y]$. Geometrically, the finiteness condition means that every time we get the same number of points on $y^2 - x^3y - 1$ for any fixed x (up to multiplicity). This is not true for a fixed y.*

We can now show the commutative algebra result using Noether normalization. By it there exist $y_1, \ldots, y_m$ such that A is finite over $k[y_1, \ldots, y_m]$. Thus, by lemma 4, $k[y_1, \ldots, y_m]$ is a field, which can only be the case if $m = 0$, so A is finite as an algebra over k. Thus, every element in A is algebraic over k.

"The elephant is not a field, unless it's not an elephant... You like the elephant? Everybody likes elephants, have you seen an elephant?"

To prove Noether Normalization we need yet another lemma:

Lemma 2.5. *Take $f \neq 0 \in k[x_1, \ldots, x_n]$, $\deg f = d$. There exists a change of variable*

$$x_1' = x_1 - \alpha_1 x_n, \ldots, x_{n-1}' = x_{n-1} - \alpha_{n-1}x_n, x_n' = x_n$$

such that $f(x_1' + \alpha_1 x_n, \ldots, x_{n-1}' + \alpha_{n-1}x_n, x_n)$ has a term cx_n^d with $c \neq 0$.

Proof. Write $f = f_0 + f_1 + \cdots + f_d$ where f_i is a homogeneous degree i polynomial. Then, f_d is non-zero, so there exist α_i such that $f_d(\alpha_1, \ldots, \alpha_{n-1}, 1)$, the coefficient of x_n^d, is non-zero. □

Proof (Of Noether Normalization): By induction, $A[a_1, \ldots, a_n]$ finitely generated. Consider $k[x_1, \ldots, x_n] \xrightarrow{\varphi} A$ be a surjective homomorphism. If $I = \ker \varphi = 0$ we are done. If $I \neq 0$, consider $f \neq 0 \in I$. Base case $n = 1$: $A = k[a]$, $f(a) = 0$ implies a is integral over k. Thus $k[a] - k$ is finite. Assume for $n - 1$ this is known, take $k[a_1, \ldots, a_n]$. Choose $\alpha_1, \ldots, \alpha_{n-1}$

so $f(x_1' + \alpha_1 x_n, \ldots, x_{n-1}' + \alpha_{n-1}x_n, x_n)$ has a non-zero x_n^d term, so $a_1' = a_1 - \alpha_1 a_n$, ..., $a_{n-1}' = a_{n-1} - \alpha_{n-1}a_n$. As such,

$$\frac{1}{c} f(a_1' + \alpha_1 a_n, \ldots, a_n) = 0$$

Hence a_n is a root of a monic polynomial with coefficient in $k[a_1', \ldots, a_{n-1}']$. Hence, $k[a_1, \ldots, a_n] - k[a_1', \ldots, a_{n-1}']$ is finite, using the inductive assumption, but now we can find $k[y_1, \ldots, y_m]$ such that $k[a_1, \ldots, a_n] - k[y_1, \ldots, y_m]$ is finite. □

Definition 2.7. *If X is an afffine algebraic set $\subset \mathbb{A}^n$, a function $f : X \to k$ is called **regular** or "polynomial" if there exists $F \in k[x_1, \ldots, x_n]$ such that for all $a = (a_1, \ldots, a_n) \in X$ we have $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$.*

Example. *Consider $X \subset \mathbb{A}^2$, $X = V(y - x^2)$. Then we have $f(x, y) = x^3 + y$ which "equals" $xy + y$ on X.*

Regular functions on X form a k-algebra, taking $k[X]$ to be the coordinate ring of X, $k[x_1, \ldots, x_n] \to k[X]$ has kernel $I(X)$. So coordinate ring of X is $k[x_1, \ldots, x_n]/I(X)$.

Example. $k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$. *Then functions on the circle $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ which "equals" $\mathbb{C}[\sin t, \cos t] = \mathbb{C}[e^{it}, e^{-it}]$, so should be true that $\mathbb{C}[u, v]/(uv - 1)$. This is indeed true, and nothing more than the statement that every circle and hyperbola are isomorphic over the complex numbers.*

Facts:

1. $k[x] = k[x_1, \ldots, x_n]/I(X)$ such that $I = \sqrt{I}$. So in the quotient there are no nilpotents $a^m = 0$ or $a \neq 0$. Thus this algebra is reduced.
2. X is irreducible if and only if $I(X)$ is prime if and only if $k[x]$ is a domain.
3. X is a point if and only if $I(X)$ is maximal iff $k[X] = k$.

2.4 Lecture 11

Today we wil talk about the category of affine algebraic varieties and its equivalence to the category of reduced finitely generated k-algebras.

Reminder: a category is a set of objects, and morphisms between them. So for any two objects X, Y there is a set of morphisms $\mathrm{Mor}(X, Y)$. Note that in $\mathrm{Mor}(X, X)$ there is a designated element called the identity id_X. Also, there exists a composition operation $\circ : \mathrm{Mor}(X, Y) \times \mathrm{Mor}(Y, Z) \to \mathrm{Mor}(X, Z)$ that is associative and respects identity, so $(f \circ g) \circ h = f \circ (g \circ h)$ and $f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f$.

As an example, for any group you can take the elements of the group g as morphisms from the same object, and define composition $g \circ h = gh$ using group multiplication. The identity element e acts as the identity morphism on the object.

Now, take k to be an algebraically closed field. Take a category in which affine algebraic varieties $X = V(I) \subset \mathbb{A}^n$ with I an ideal of $k[x_1, \ldots, x_n]$ for some n are the objects. Take

the morphisms $f : X \to Y$ of these affine algebraic varieties, called either **regular maps** or **polynomial maps**, to be such that there exist $P_1, \dots P_m \subset k[x_1, \dots, x_n]$ so that for any $(b_1, \dots, b_n) \in X$, $f(X) = (P_1(b_1, \dots, b_n), \dots, P_m(b_1, \dots, b_n))$. One example of a regular map is something like $x \mapsto (x^3+1, x^2)$ between $X = \mathbb{A}^1 \to Y = \mathbb{A}^2$. ANother one is $(x_1, x_2) \mapsto x_1$. Taking X to be the parabola $y = x^2$, the morphism $(x, y) \mapsto x$ maps X to Y being the x-axis.

In this category, the identity morphism is given by $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_n)$. A composition of regular maps is again a regular map.

In any category there's a notion of an isomorphism, namely $f \in \mathrm{Mor}(X, Y)$ is an isomorphism if there exists a $g \in \mathrm{Mor}(Y, X)$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. For example, the morphism $(x, y) \mapsto x$ from a parabola to the x-axis is an isomorphism, since g from the axis to the parabola given by $x \mapsto (x, x^2)$ is its 'inverse'.

Here is a conjecture, which "will certainly give you a professor position here if you solve it". Take isomorphisms $\mathbb{A}^n \to \mathbb{A}^n$ in the category of affine algebraic sets. For instance, take $(x, y) \mapsto (x^2 + y, x)$, its inverse is $(x, y) \mapsto (y, x - y^2)$. Notice that the determinant of the Jacobian of an isomoprhism is a non-zero constant, the converse, that it suffices for a regular map to have a non-zero constant Jacobian in order for it to be invertible, is called the Jacobian conjecture.

Let $X \subset \mathbb{A}^n$ be an affine algebraic variety, then $k[X] = k[x_1, \dots, x_n]/I(X) = \mathrm{Mor}(X, \mathbb{A}^n)$. Note that $k[X]$ is a finitely generated algebra over k, and $k[X]$ is **reduced**, i.e. has no nilpotent elements, which happens iff $I(X) = \sqrt{I(X)}$.

Consider now the category of reduced finitely generated algebras over k. Morphisms $\mathrm{Mor}(B, A)$ in this category being homomorphisms of k-algebras $B \to A$. Some examples:

1. $\mathbb{C}[x] \to \mathbb{C}$ via $x \mapsto 3$.
2. $\mathbb{C}[y] \to \mathbb{C}[x, y]/(y^2 - x)$ via inclusion.
3. $\mathbb{C}[x, y]/(x^2 + y^2 - 1) \to \mathbb{C}[t_1, t_2]/(t_1 t_2 - 1)$ so this is an isomorphism in the category.

We want to say that these categories are in some way the same. For this, define a map $F : \mathcal{C} \to \mathcal{D}$ between categories, called a **functor**. For any object $X \in \mathcal{C}$, a functor F gives an object $F(X) \in \mathcal{D}$. For any morphism $f : X \to Y$ we have a map $F(f) : F(X) \to F(Y)$.

Let a (contravariant) functor between the category of affine algebraic varities and finitely generated algebras over k be given by $k[X] = k[x_1, \dots, x_n]/I(X)$. This functor takes a map $f : X \to Y$ given by $(x_1, \dots, x_n) \mapsto (F_1(x_1, \dots, x_n), \dots, F_m(x_1, \dots, x_n))$ to the map $k[Y] = k[y_1, \dots, y_m]/I(X) \to k[X] = k[x_1, \dots, x_n]/I(X)$ by $y_i \to F_i(x_1, \dots, x_n)$.

Some examples:

1. The example of isomorphism between parabola and the x-axis corresponds to the map $\mathbb{C}[x] \to \mathbb{C}[x, y]/(y - x^2)$.
2. A map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $x \mapsto (x, 3x - 1)$ corresponds to $\mathbb{C}[x, y] \to \mathbb{C}[x]$ by $x \mapsto x$, $y \mapsto 3x - 1$.

The most straightforward way to think of how to say that these two categories are equivalent is to come up with another functor G such that $F \circ G = \mathrm{id}_{\mathcal{C}}$, $G \circ F = \mathrm{id}_{\mathcal{D}}$. However this almost never makes sense, the map in the other direction will involve choices and not be well-defined.

The correct notion is the equivalence of categories. So, a functor F gives an equivalence if there exists a natural transformation $F \circ G \to \mathrm{id}$, and in the other direction also. (We won't talk about what that means, watch Bouchard's category theory videos). Instead we will prove some facts about F that should make it clear that it defines an equivalence.

Proposition 2.4. *F is **essentially surjective**: For every finitely generated algebra A there exists an affine algebraic variety X s.t. $k[X] \cong A$, finitely generated implies $A \cong k[x_1, \ldots, x_n]/I = k[X]$, A is reduced implies for $V(I) = X \subset \mathbb{A}^n$, $I = \sqrt{I}$. (TODO)*

Proposition 2.5. *F is **fully faithful**: the map $\mathrm{Mor}(X, Y) \to \mathrm{Hom}(k[Y], k[X])$ given by $f \mapsto f^*$ given by F is a bijection.*

Indeed, for any map $k[y_1, \ldots, y_m]/I(Y) \to k[x_1, \ldots, x_n]/I(X)$ by $y_i \mapsto P_i$, then take $X \to Y$ via $(x_1, \ldots, x_n) \mapsto (P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$.

These two facts give us what we want by the following theorem:

Theorem 2.7. *If $\mathcal{C}$ and $\mathcal{D}$ are categories, $F : \mathcal{C} \to \mathcal{D}$ Then F is an equivalence of categories if and only if F is fully faithful and essentially surjective.*

2.5 Lecture 12

In analysis you studied the tangent space to a manifold at a point. We want to talk about this concept for algebraic varieties. Let $X \subset \mathbb{A}^n$, $p \in X$. We want to define $T_pX \subset \mathbb{A}^n$ an affine subspace. Our eventual goal is to define this space in terms of $k[X]$, the ring of functions on X.

Let k be a char 0, algebraically closed field. Consider $X \subset \mathbb{A}^n$, $p = (0, \ldots, 0)$, $a \in (a_1, \ldots, a_n) \in \mathbb{A}^n$. Suppose $I(X) = (f_1, \ldots, f_m)$. Then consider a line $L_a = \{(ta_1, \ldots, ta_n) \mid t \in k\}$. In this case $X \cap L_a = \{t \mid \{f_1(ta_1, \ldots, ta_n) = 0, \ldots, f_m(ta_1, \ldots, ta_n) = 0\}\}$. Let $f(t)$ be the GCD of f_i in that system, so $X \cap L_a$ are the roots of $f(t)$. Note $p \in X$ means $t = 0$ is a root of $f(t)$, and L_a being tangent to X at p means $t = 0$ is in fact a double root, i.e. $t^2 \mid f(t)$. Thus, $t^2 \mid f(t)$ implies $t^2 \mid f_i(ta_1, \ldots, ta_m)$ for all generators f_i of $I(X)$.

Reminder of Taylor's formula for polynomials at p:

$$F(x_1, \ldots, x_n) = F(p) + \sum \frac{\partial F}{\partial x_i}(p)(x_i - p_i) + \sum \frac{\partial F}{\partial x_i \partial x_j}(p)(x_i - p_i)(x_j - p_j) + \ldots$$

(number of sums finite because F has derivatives only as high as its degree). Denote by d_pF the first sum above after $F(p)$. Then, $t^2 \mid f_i(ta_1, \ldots, ta_n) = 0 + [\frac{\partial f_i}{\partial x_i} ta_i + \ldots] + \frac{\partial f_1}{\partial x_i x_j} t^2 a_1 + \ldots$. In other words, $d_p f_i(a_1, \ldots, a_n) = 0$ for $1 \leq i \leq m$.

Definition 2.8. *For $X \subset \mathbb{A}^n$, $p \in X$, $T_pX = V(d_pf \mid f \in I(X))$.*

This is an affine subspace, and a vector space of dimension $\leq n$.

Theorem 2.8. *For an affine algebraic variety $X \subset \mathbb{A}^n$ (and $p = (p_1, \ldots, p_n) \in X$), $k[X] = k[x_1, \ldots, x_n]/I(X)$, let $\mathfrak{m}_p$ be the regular functions on X vanishing at p. There exists a canonical isomorphism*

$$(T_pX)^* \cong \mathfrak{m}_p/\mathfrak{m}_p^2$$

Proof. Functions in $\mathfrak{m}_p$ are $f \in k[X]$ such that $f(p) = 0$ and $f = F(x_1, \ldots, x_n) \mid_x$ (so $F(p_1, \ldots, p_n) = 0$). We send every such f to the linear function d_pF on $\mathbb{A}^n$. This map is well defined, since indeed if $\tilde{F} \mid_X = F \mid_X$ we know $\tilde{F} = F + g_1 f_1 + \cdots + g_m f_m$. But then

$$d_p\tilde{F} = d_pF + f_1(p)d_pg_1 + \cdots + f_m(p)d_pg_m + g_1(p)d_pf_1 + \cdots + g_m(p)d_pf_m$$

But $f_i(p) = 0$, so $d_p\tilde{F} \mid_{T_pX} = d_pF \mid_{T_pX}$.

So this map $d_p : \mathfrak{m}_p \to (T_pX)^*$ is well-defined, linear, and $\mathfrak{m}_p^2 \subset \ker d_p$ (since $d_p(F_1F_2) = F_1(p)d_pF_2 + F_2(p)d_pF_1 = 0$), so we have a linear map $\mathfrak{m}_p/\mathfrak{m}_p^2 \to (T_pX)^*$. This is surjective because for any linear function $\lambda(x_1 - p_1) + \cdots + \lambda_n(x_n - p_n) \in (T_pX)^*$, we have $d_p(\lambda(x_1 - p_1) + \cdots + \lambda(x_n - p_n))$ equals to it. The map is also injective since if $d_pF = 0$ we have $F = \sum(...)x_ix_j + \sum(...)x_ix_jx_k + \ldots$ i.e. $F \in \mathfrak{m}_p^2$. □

Another way to understand this is to try to understand if $T_pX \cong (\mathfrak{m}_p/\mathfrak{m}_p^2)$, i.e. can you find a pairing $T_pX \otimes (\mathfrak{m}_p/\mathfrak{m}_p^2) \to k$? Yes, the directional derivative D_vf.

Let's briefly talk about local rings. Recall that X is irreducible iff $I(X)$ is prime iff $k[X]$ is an integral domain (TODO?). Note the field of fractions $\mathrm{Frac}(k[X]) = k(X)$. For example $k(\mathbb{A}^n)$ is the set of all P/Q where $P, Q \in k[X]$ with $Q \neq 0$. On the other hand $k[X]$ are restrictions of rational functions P/Q on $\mathbb{A}^n$ such that $Q \mid_X = 0$. Note $k(X) \subset k(\mathbb{A}^n)$.

Definition 2.9. *The **local ring** $\mathcal{O}_p$ is the subring of $k(X)$ consisting of $(F/G) \mid_X$ where $G(p) \neq 0$.*

So for $X \in \mathbb{A}^2$, $\mathcal{O}_{(0,0)} = \{\frac{F(x,y)}{G(x,y)} \mid G(0,0) \neq 0\}$. So $\frac{x+y}{1+x}$ is ok, $\frac{x^2+y^2}{xy}$ is not.

Lemma 2.6. *$\mathcal{O}_p$ has a unique maximal ideal.*

Consider $\{F/G \mid F(p) = 0, G(p) \neq 0\} = \mathfrak{m}_p\mathcal{O}_p$, every element in $\mathcal{O}_p \setminus (\mathfrak{m}_p\mathcal{O}_p)$ is invertible, so $\mathfrak{m}_p\mathcal{O}_p$ is maximal.

Another good fact is $(T_pX)^* = (\mathfrak{m}_p\mathcal{O}_p)/(\mathfrak{m}_p\mathcal{O}_p)^2$.

The intersection number $I_p(X, Y) = \dim_{\mathbb{C}} \frac{\mathcal{O}_p\mathbb{A}^2}{(f(x,y),g(x,y))}$.

2.6 Lecture 13

Definition 2.10. *If X is irreducible, then the **dimension** of X is the minimum of all dimensions of its tangent spaces T_pX. If $X = \cup X_i$, a union of irreducible spaces, then the dimension of X is* $\max_i \dim X_i$.

Consider the sets $S_0(X) \supset S_1(X) \supset \ldots$ where $S_r(X) = \{p \in X \mid \dim T_pX \geq r\}$.

Lemma 2.7. *$S_r(X)$ is closed in the Zariski topology.*

Proof. Note that if $I(X) = (f_1, \ldots, f_m)$ we have $T_pX = V(df_p, \ldots, d_pf_m)$, so $\dim T_pX = n - \mathrm{rank}\left[\frac{\partial f_i}{\partial x_j}\right]$. Hence $S_r(X) = \{p \in X \mid \mathrm{rank}\left[\frac{\partial f_i}{\partial x_j}\right] \leq n - r\}$, in other words, the set of all $p \in X$ such that all minors of size $n-r+1$ of the matrix $\left[\frac{\partial f_i}{\partial x_j}\right]$ vanish. Since this is given by a system of polynomial equations (determinants of minors $= 0$), this set must be closed. □

Corollary: if $X \subset$ irreducible affine algebraic set, $d = \dim X$, then there exists $U \subset X$ that is open dense set such that for every point $p \in U$, $\dim T_p X = \dim X$. These points are called **smooth**.

Definition 2.11. *A **quasiaffine algebraic variety** is any intersection $X \cap U$ of a (Zariski) closed $X \subset \mathbb{A}^n$ and a (Zariski) open set $U \subset \mathbb{A}^n$.*

We can define an analogous thing for $\mathbb{P}^n$, giving it the Zariski topology of solution sets of systems of homogeneous polynomials.

Definition 2.12. *A **quasiprojective variety** is an intersection of a closed set in $\mathbb{P}^n$ with an open one.*

Here is another definition of dimension: Let X be an irreducible affine algebraic variety. Then we have a tower $k(X) - k[X]$. Recall that $t_1, \ldots, t_m \in k(X)$ are called *algebraically independent* if $F(t_1, \ldots, t_m) = 0$ with F a polynomial implies $F = 0$ (actually should be a rational function but here saying polynomial is fine). Then, $t_1, \ldots, t_m$ is a **transcendence basis** if they are algebraically independent, and for any $t \in k(X)$, $t, t_1, \ldots, t_m$ are algebraically dependent.

We have a similar result to one in linear algebra:

Theorem 2.9. *Every two transcendence bases have the same cardinality.*

Example.

1. *$\mathbb{A}^n$, then $k(\mathbb{A}^n) = k(x_1, \ldots, x_n)$, transcendence degree n.*
2. *$X = V(y^2 - x^3 + 1)$, then $k[X] = k[x, y]/(y^2 - x^3 + 1)$, there is a tower over $k[X]$, and also $k[X] = k(X)[y]/(y^2 - x^2 + 1)$, note that x is then a transcendence basis of this field.*
3. *X a hypersurface in $\mathbb{A}^n$ given by $f(x_1, \ldots, x_n) = 0$. So, considering $k[x_1, \ldots, x_n]/(f(x_1, \ldots, x_n))$, $(k[x_1, \ldots, x_{n-1}][x_n]/(f)) - k(x_1, \ldots, x_{n-1})$, hence the transendence degree of $k(X)$ is $n - 1$*

Theorem 2.10. *For X irreducible affine algebraic variety, $\min\{\dim T_p X \mid p \in X\}$ = transcendence degree of $k(X)$.*

The proof is via rational maps.

Definition 2.13. *A map $\varphi \in k(X)$ for X irreducible affine algebraic variety is **regular** at $p \in X$ if $\varphi = f/g$, with $f, g \in k[X]$ and $g(p) \neq 0$.*

Example. *Take a circle $X = V(x^2 + y^2 - 1)$, and take a function $\frac{y-1}{x}$, which we can take to be in $k(X)[y]/(y^2 + x^2 - 1)$, so $\varphi = \frac{-x}{y+1}$ gives us the same function on X where both are defined, except the latter is defined everywhere except at the bottom point of the circle. So φ is regular everywhere except $(0, -1)$.*

Last time we defined $\mathcal{O}_p$ to be the set of all functions that are regular at p.

Theorem 2.11. *For X an affine algebraic variety,*

$$k[X] = \cap_{p \in X} \mathcal{O}_p$$

Proof. One direction is obvious. Now suppose $\varphi \in k(X)$ is in every $\mathcal{O}_p$, so for any p there exist $f_p, g_p \in k[X]$ such that $\varphi = \frac{f_p}{g_p}$ with $g_p(p) \neq 0$. Consider the ideal I generated by all g_p for varying $p \in X$. Then $V(I) = \emptyset$, if not there is a $q \in V(I)$, for all $p \in X$, $g_p(q) = 0$, but what if $p = q$? Hence, applying Nullstellensatz, $I = k[X]$, and so $k[X] \ni 1 = u_1 g_{p_1} + u_2 g_{p_2} + \cdots + u_k g_{p_k}$. Then

$$\varphi = \varphi \cdot (u_1 g_{p_1} + u_2 g_{p_2} + \cdots + u_k g_{p_k}) = u_1 f_{p_1} + \ldots u_k f_{p_k} \in k[X]$$

□

[Proof might be on the final]

For $\varphi \in k(X)$, let the *domain* $D(\varphi) := \{p \in X \mid \varphi \text{ is regular at } p\}$. Then $D(\varphi)$ is open and dense in X, since $D(\varphi) = \bigcup\{g \neq 0\}$ where the union is over all possible g in the presentation $\varphi = f/g$. We can redefine the field of fractions in terms of regular maps:

$$k(X) = [U, \varphi]/([U_1, \varphi_1] \sim [U_2, \varphi_2])$$

Where $\varphi : U \to \mathbb{A}^1$ is a regular function on its open domain U, and functions are identified if they are equal on the intersections of their domains. Showing this is equivalent to an old definition is left as an exercise.

Definition 2.14. *If X and Y are irreducible affine varieties, $\varphi : X \subset \mathbb{A}^n \to Y \subset \mathbb{A}^m$ is **rational** if $\varphi = (\varphi_1, \ldots, \varphi_m)$ where $\varphi_i \in k(X)$. For all $p \in \cap D(\varphi_i)$, $(\varphi_1(p), \ldots, \varphi_m(p)) \in Y$.*

Some examples include stereographic projections.

2.7 Lecture 14

Example. *Consider $\mathbb{A}^2 \to \mathbb{A}^2$ given bt $(x, y) \mapsto \left(\frac{x}{y^2-x-1}, \frac{7x}{y^2-x-1} + 1\right)$. This is defined everywhere except on $y^2 - x - 1 = 0$*

Note that we cannot compose rational maps to get rational maps. Say in the example above we can't compose it with $\frac{x^2+y^2}{y-7x-1}$. In order to get composable rational maps we need to introduce:

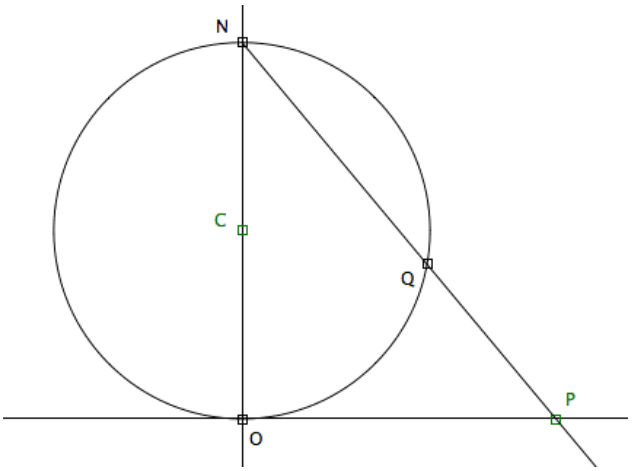
Definition 2.15. *φ is called **dominant** if $\overline{\varphi(X)} = Y$ (closure in the Zariski topology).*

Then you have a category of irreducible affine algebraic sets and dominant maps. Given X and Y and a dominant map f between them, a priori we get a map $f^* : k[Y] \to k(X)$. However, because f is dominant, we must have that f^* is injective, so f^* can be extended to a map of the field of fractions, we thus out of f get a map $f^* : k(Y) \to k(X)$. Hence, we get an equivalence of the category of irreducible affine algebraic sets and dominant maps with the category of finitely generated fields over k and injections between them. Note that the category of sets and rational maps between them doesn't change if you replace "irreducible affine algebraic sets" with "projective" or "quasiprojective" sets.

Because we have this equivalence, we can think of a way to define isomorphisms in the former category. Namely a **birational isomorphism** $\varphi : X \to Y$ between irreducible affine

algebraic sets is a (dominant) rational map such that there is a (dominant) rational map $\psi : Y \to X$ that acts as the inverse for φ.

Important example of a birational isomorphism is a stereographic projection. In the picture above, we send $Q \in C$ to $P \in \mathbb{A}^1$. N gets sent to ∞. Writing this map explicitly is an expercise.



We also have the isomorphism $k(x)[y]/(x^2+y^2-1) \to k(t)$ which sends $x \mapsto \frac{2t}{t^2+1}$ and $\frac{t^2-1}{t^2+1}$. This has the inverse map $t \mapsto \frac{1+y^2}{x}$ (TODO: might be wrong, exercise to figure out).

Now we consider cubic curves. There will be two types of them up to isomorphism, cusps with equations $zx^2 = y^3$, and nodal with equation $zy^2 = zx^2 - x^3$. A generic line crossing a cusp will cross it in three points, in the other cases some intersections will be counted with multiplicity (except in some cases, will talk about this more next time). Similarly we define intersection multiplicity on a cubic. There is a birational isomorphism between a cusp $\mathbb{P}^1$ and a cusp X given by $t \mapsto (t^3, t^2) \in \mathbb{A}^2$. In the other category, the inverse to this is given by $k(t) \to k[x](y)/(x^2 - y^3)$ given by $t \to x/y$, so $y = t^2$ and $x = t^3$.

Proposition 2.6. *Every affine (projective) algebriac variety is birationally isomorphic to a hypersurface in* $\mathbb{A}^n$.

Proof. If we have $k[X] - k[t_1, \ldots, t_m]$ is a finite algebra, we have that $k(X) - k(t_1, \ldots, t_m)$ is a finite degree extension. By the primitive element theorem, if your field F is characteristic 0, we have $L - F$ finite means there is an element α such that $L = F(\alpha)$ □

Proposition 2.7. *If* $X \sim Y$ *(birationally isomorphic) then* $\dim X = \dim Y$ *(via tangent spaces).*

Proof. Recall that for X an irreducibel aglebraic variety $T_pX \cong [\mathfrak{m}_p/\mathfrak{m}_p^2]^\vee$. Let $X_{\text{sm}} \subset X$ be the set of points $p \in X$ for which $\dim T_pX = \dim X$. Then for $\varphi : X \to Y$, and we know since φ is dominatnt $\overline{\text{Im}(D(\varphi))} = Y$ (similar for ψ), and also there exist $p \in D(\varphi)$ and $\varphi(p) \in D(\psi)$ such that $p \in X_{\text{sm}}$ and $\varphi(p) = Y_{\text{sm}}$. Hence, if $k(X) \cong k(Y)$, local rings are isomorphic, so $(\mathfrak{m}_p/\mathfrak{m}_p^2)^\vee \cong (\mathfrak{m}_{\varphi(p)}/\mathfrak{m}_{\varphi(p)}^2)^\vee$, hence dimensions are the same. □

Fact 2.1. *If* X *is an irreducible affine algebraic variety we have that* $\dim T_pX$ *is equal to the transcendence degree of* $k(X)$.

One more definition of dimension:

Definition 2.16. *Consider for an affine irreducible set X we have a chain of closed proper sets:*

$$X \supsetneq X_1 \supsetneq X_2 \cdots \supsetneq X_n \supsetneq \emptyset$$

If this is the maximal-length chain, then n gives the ***Krull dimension*** *of X.*

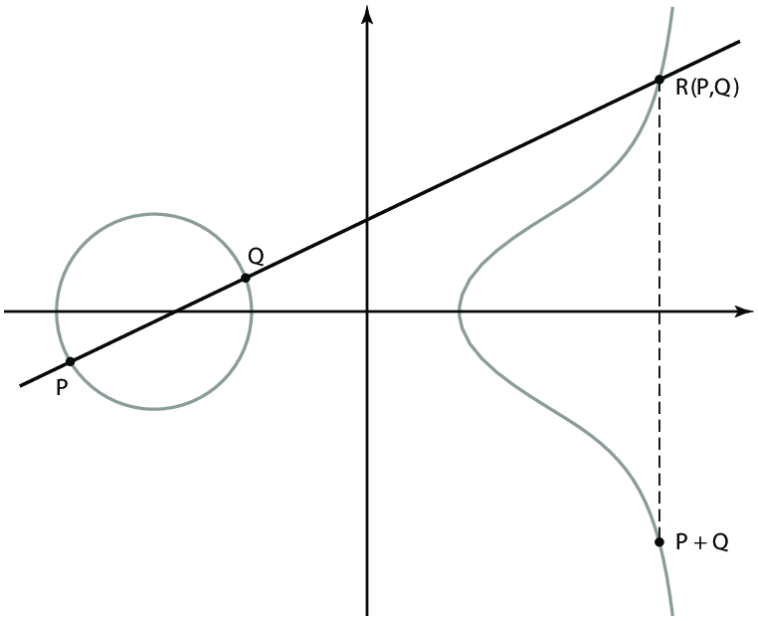
Proving that this is equivalent to the previous definitions is difficult.

Suggested further action: if you're abitious, read the first part Shafarevich, chapters 1, 2, 3. This gives a very good classical foundation in the subject. Most people read Harthshorne for the scheme theory, but it's easier to get intuition from Shafarevich. After this course you should be able to read those chapters pretty comfortably. After that, there are two big sources of examples: curves and surfaces.We will talk about curves for the remainder of the course.

2.8 Lecture 15

We will not prove Bezoiut's, we need 5 more classes for that. Let's remind ourselves of what it is. Let C be a projective variety in C, defined by the vanishing set of a homogeneous polynomial $F(x, y, z)$ of degree d. If $d = 1$, C is a line, $d = 2$ means C is a pair of lines or a conic, $d = 3$ is as we will discuss an elliptic curve (or otherwise something not smooth).

We will show that points on an elliptic curve form a group, under the following addition law: (we are adding P and Q)



Bezoiut's theorem: suppose C_1 and C_2 are projective curves on $\mathbb{P}^2$ with no common irreducible components. Then,

$$\sum_{P \in \mathbb{P}^2} I_P(C_1, C_2) = \deg(C_1) \deg(C_2)$$

Where I_P is the intersection multiplicity of C_1 and C_2 at P. Goal is not to prove this theorem but to define the "intersection multiplicity" well.

Definition 2.17. *Consider two curves $C_1, C_2 \subset \mathbb{A}^2$, C_1 given by $f(x,y) = 0$ and C_2 given by $g(x,y) = 0$. Then the **intersection number** of C_1 and C_2 at a point $P \in \mathbb{A}^2$ is*

$$I_P(C_1, C_2) = \dim \frac{\mathcal{O}_{\mathbb{A}^2,P}}{(f,g)}$$

Reminder: $\mathcal{O}_{\mathbb{A}^2,P}$ (denoted also $\mathcal{O}_P$) is the set of all $\frac{u(x,y)}{v(x,y)}$ with $u, v, \in k[x,y]$, $v(P) \neq 0$. This has a unique maximal ideal $\mathfrak{m}_P = \{u/v \mid v(P) = 0, u(P) \neq 0\}$. Hence, $\mathcal{O}_P/\mathfrak{m}_P \cong k$ for example. dim above is defined to be the transcendence degree.

Example. *We have that $\mathcal{O}_{\{0\}}/(x,y) = k$ since (x,y) is precisely the maximal ideal of the local ring, hence the interesection number of the x and y axes is 1.*

Proposition 2.8. *$I_P(C_1, C_2) \geq 1$ if and only if $P \in C_1 \cap C_2$.*

Proof. If $P \neq C_1$, then $f(P) \neq 0$ (C_1 defined by $f = 0$), so $f \in \mathcal{O}_P$, and similarly $g \in \mathcal{O}_P$. As such $(f,g) = \mathcal{O}_P$ and $\dim \mathcal{O}_P/(f,g) = 0$.

On the other hand if $P \in C_1 \cap C_2$ then $f(P) = g(P) = 0$, hence $\mathfrak{m}_P = (f,g)$. Thus $\dim \mathcal{O}_P/(f,g) \geq \dim \mathcal{O}_P/\mathfrak{m}_P = 1$. □

Proposition 2.9. *The intersection number $I_P(C, L)$ of a curve given by $f = 0$ and a line L, is equal to the multiplicity of P as a root of $f\mid_P$.*

We consider the multiplicity of P since plugging in linear expressions for x, y makes f a polynomial in one variable.

Proof. WLOG set $P = (0,0)$ and $L = \{y = 0\}$. Then considering

$$f(x,y) = a_0 + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + \dots$$

we get

$$f\mid_L = a_0 + a_{1,0}x + a_{2,0}x^2 + \cdots = a_k x^k + \cdots = x^k(1 + x + x^2 + \dots)$$

where a_k is the first non-zero coefficient, so $\text{mult}_0 f\mid_L = k$.

The thing in parens is a unit, so $(f(x,y), y) = (f\mid_L, y) = (x^k, y)$. Since $\mathcal{O}_0/(x^k, y)$ has basis $1, x, x^2, \dots, x^{k-1}$, we know that its dimension is k. □

Definition 2.18. *C_1 and C_2 intersect **transversally** at P if*

1. *C_1 and C_2 are smooth at P.*
2. *$(T_P C_1) \cap (T_P C_2) = \{P\}$.*

Theorem 2.12. *C_1 and C_2 intersect at transversally at P if and only if $I_P(C_1, C_2) = 1$.*

To prove this we need to consider the certain form of Nakayama lemma.

Lemma 2.8 (Nakayama)**.** *Let A, B be algebras, A is finite over B. If $A \neq 0$ and $I \subsetneq B$ is a proper ideal. Then $IA \subseteq A$.*

Proof. Since A is fininte over B, $A = a_1B + \dots a_nB$ for some elements $a_i \in A$. Suppose for contradiction $IA = A$, then

$$\begin{cases} a_1 = a_1\lambda_{11} + \cdots + a_n\lambda_{n1} \\ a_2 = a_1\lambda_{12} + \cdots + a_n\lambda_{n2} \\ \dots a_n = a_1\lambda_{1n} + \cdots + a_n\lambda_{nn} \end{cases}$$

where all λ's are in $I \subset B$. Rearranging we get the system

$$\begin{bmatrix} \lambda_{11} - 1 & \dots & \lambda_{n1} \\ \vdots & \ddots & \vdots \\ \lambda_{1n} & \dots & \lambda_{nn} - 1 \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = 0$$

Hence the determinant of the coefficient matrix has to be zero, in other words, via definition of determinant we then get that $1 \in I$, but this would mean $I = B$, contradiction. □

Proposition 2.10. *Let X be an affine variety. Recall $\mathfrak{m}_P/\mathfrak{m}_P^2 = (T_PX)^*$. Let $f_1, \dots, f_n \in \mathfrak{m}_P$. Then $(f_1, \dots, f_n) = \mathfrak{m}_P$ iff $\overline{f_1}, \dots, \overline{f_n}$ span $\mathfrak{m}_P/\mathfrak{m}_P^2$.*

The forward direction is very clear, the reverse is surprising:

Proof. Let $B = \mathcal{O}_P/(f_1, \dots, f_n)$, it contains $\mathfrak{m}_P$. Let $A = \mathfrak{m}_P/(f_1, \dots, f_n)$, indeed A is finite over B. We prove this proposition by contradiction, suppose $(f_1, \dots, f_n) \subsetneq \mathfrak{m}_P$, then $A \neq 0$, and by Nakayama $\mathfrak{m}_P(\mathfrak{m}_P/(f_1, \dots, f_N))$ which is a proper subset of $\mathfrak{m}_P/(f_1, \dots, f_n)$. Then for any $x \in \mathfrak{m}_P/(f_1, \dots, f_n)$, since $f_1, \dots, f_n$ span $\mathfrak{m}_P/\mathfrak{m}_P^2$, $x = u_1f_1 + \dots u_nf_n$, so $x \in \mathfrak{m}_P(\mathfrak{m}_P/(f_1, \dots, f_n))$, contradiction. □

We can now prove theorem 2.12:

Proof. First suppose $I_P(C_1, C_2) = 1$. Then $\dim \mathcal{O}_P/(f, g) = 1$. Then $f(P) = g(P) = 0$. Then $f = ax + by + \dots$ and $g = cx + dy + \dots$. Hence if $(f, g) \subset \mathfrak{m}_P$, $\overline{f}, \overline{g} \in \mathfrak{m}_P/\mathfrak{m}_P^2$. Dimension of this ring $= 1$ iff $(f, g) = \mathfrak{m}_P$, hence $\langle \overline{f}, \overline{g} \rangle = \mathfrak{m}_P/\mathfrak{m}_P^2$. The other direction is given by the fact that since $\overline{f}$ and $\overline{g}$ are non-zero, in the expression for f and g above $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0$ (since that's the only way lines intersect transversally). (TODO) □

We will now talk about cubic curves and addition law on elliptic curves.

Theorem 2.13 (Calyey-Bacharach)**.** *For $C_1, C_2 \in \mathbb{P}^2$ cubic curves intersecting at 9 distinct points $P_1, \dots, P_9$, suppose that a cubic curve C contains all $P_1, \dots, P_8$. Then $C \ni P_9$.*

Proof. (Proof in Tau) Space of cubic curves $\mathbb{P}^9 = \mathbb{P}[\mathbb{S}^3V^2]^{X^aY^bZ^c}$ $(a + b + c = 3)$. The set of cubic curves passing through a particular point P is a hyperplane H_P in $\mathbb{P}^5$. We claim that $\bigcap_{i=1}^8 H_{P_i} = \mathbb{P}^1$. This implies the theorem since then indeed $C = \lambda C_1 + \mu C_2$ and so $C(P_9) = \lambda C_1(P_9) + \mu C_2(P_9) = 0$.

Indeed, suppose $\dim \cap_{i=1}^{8} H_{P_i} \geq 2$, so for any two points $X, Y \in \mathbb{P}^2$ there is a cubic containing $P_1, \ldots, P_8, X, Y$. Step 1: No eight four points out of $P_1, \ldots, P_8$ are on the same line, no 7 points are on the same quadratic curve. Step 5: Any 5 of the P_i's lie on a unique quadric (if there are two distinct quadrics passing through 5 of the pts, then they must intersect in an irreducible component so both are a union of two lines, and this is unique since no 4 points lie on a line). The rest of the steps are casework on how many points can like on what components of some cubic (TODO). □

3 Lecture 16: Addition Laws

3.1 Addition Laws

We supposedly now have the background for "real, hard" theorems in algebraic geometry.

Example. *Rudenko calls this the motivation for "real" algebraic geometry, beginning with a "baby" addition law.*

$$\int_0^y \frac{dx}{\sqrt{1-x}} + \int_0^z \frac{dx}{\sqrt{1-x^2}} = \int_0^{T(yz)} \frac{dx}{\sqrt{1-x^2}}, T(yz) = y\sqrt{1-z^2} + z\sqrt{1-y^2} = \sin(\alpha+\beta)$$

By substutiting, we have

$$\int_0^{\sin\alpha} \frac{dx}{\sqrt{1-x}} + \int_0^{\sin\beta} \frac{dx}{\sqrt{1-x^2}} = \int_0^{\sin(\alpha+\beta)} \frac{dx}{\sqrt{1-x^2}}$$

To put this in terms of differential forms, instead consider $\frac{dx_1}{\sqrt{1-x_1^2}}$*, fix* $z = c$ *to see that*

$$\frac{dx_1}{\sqrt{1-x_1^2}} = \frac{dx_2}{\sqrt{1-x_2^2}}$$

where $x_2 = x_1\sqrt{1-c^2} + c\sqrt{1-x_1^2}$

Euler expands on this additive law with

Example.

$$\frac{dx_1}{\sqrt{1-x_1^4}} = \frac{dx_2}{\sqrt{1-x_2^4}}, \quad x_2 = \frac{x_1\sqrt{1-c^2} + c\sqrt{1-x_1^2}}{1+c^2x_1^2}$$

In other words,

$$\int_0^{x_1} \frac{dx}{\sqrt{1-x^4}} + \int_0^{c} \frac{dx}{\sqrt{1-x^4}} = \int_0^{x_2} \frac{dx}{\sqrt{1-x^4}}.$$

We want to find $x_2 = f(x_1)$ s.t.

$$\frac{dx_1}{\sqrt{x_1^3+4x_1+b}} = \frac{dx_2}{\sqrt{x_2^3+4x_2+b}}, \text{ some } x_2.$$

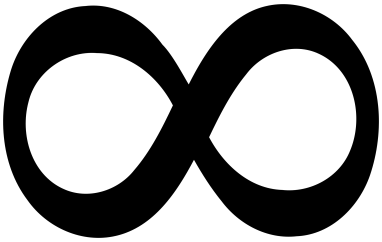


Figure 1: Graph of $y^2 = 1 - x^4$. Notice the singularity.

To formula the above in more general terms, we are looking for identities to $\frac{dx}{y}$ with $y^2 = ax^3 + ax + b$.

In the previous previous example, we had

$$y^2 = 1 - x^4$$

Theorem 3.1. *Every curve (not necessarily smooth) is blrationally isomorphic to a smooth projective curve*

$$y^2 = 1 - x^4 \to y^2 z = x^3 + ax^2 z^2 + bz^3$$

Definition 3.1. ***An elliptic curve*** *is a smooth projective cubic*

Theorem 3.2. *All elliptic curves are projectively equivalent to* $zy^2 = x^3 + axz^2 + bz^3$ *with* $4a^3 + 427b^2$.

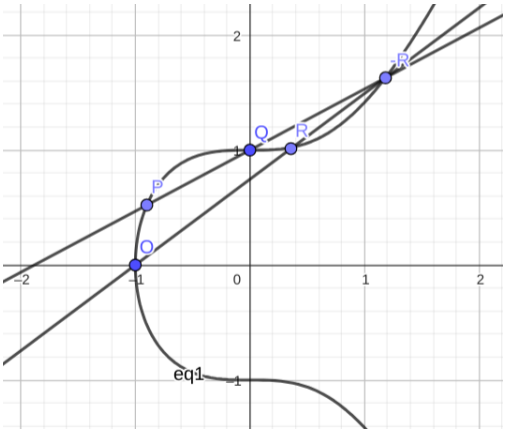
Proof. Show that every elliptic curve has a flex point (multiplicity 3) and one can map flex points to $[0 : 1 : 0]$ (form has a flex point here) □

3.2 Addition Law on Elliptic Curves

Fix $O \in E$ (point at infinity is classic, i.e. reflection over x-axis is negation). We define a map

$$E \times E \to E$$

by $(P, Q) \to R$



To show that this is a group, note that O is the identity and inverse is obvious (connect to O). Note that commutativity is also obvious.

Now for associativity:

Look at this diagram Figure 2:

E goes through all 9 points

Define the lines connecting these points:

$$\ell_1 : (P+Q)R$$
$$\ell_j : (PQ)$$
$$\ell_3 : (R+Q)(-(R+Q)).$$

$\ell_1\ell_2\ell_3$ goes through the 9 points.

Define the lines connecting these points:

$$I : P-(Q+R)$$
$$II : Q(Q+R)$$
$$III : (P+Q)O.$$

$I \cdot II \cdot III$ goes through 8 points $\implies$ goes through the 9th by Cayley-Bacharach Theorem. As this cubic is three lines, it then follows that $P, P+Q, -((P+Q)+R)$ are colinear. This suffices to show associativity.

Notice that $F+F+F=0$ for flex points. So we have an infinite group with torsion.

3.3 Differential Forms

X - alg. variety

Definition 3.2. *A **regular one-form** assigns at every point P an element in $T_p^\star = \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ This is a map $X \to \bigcup_{\in\in X} \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ (i.e. section of tangent bundle).*

For example, $f(x)dx$ returns the first coordinate and $f(x)dx+g(x,y)dy$ returns a tangent vector.

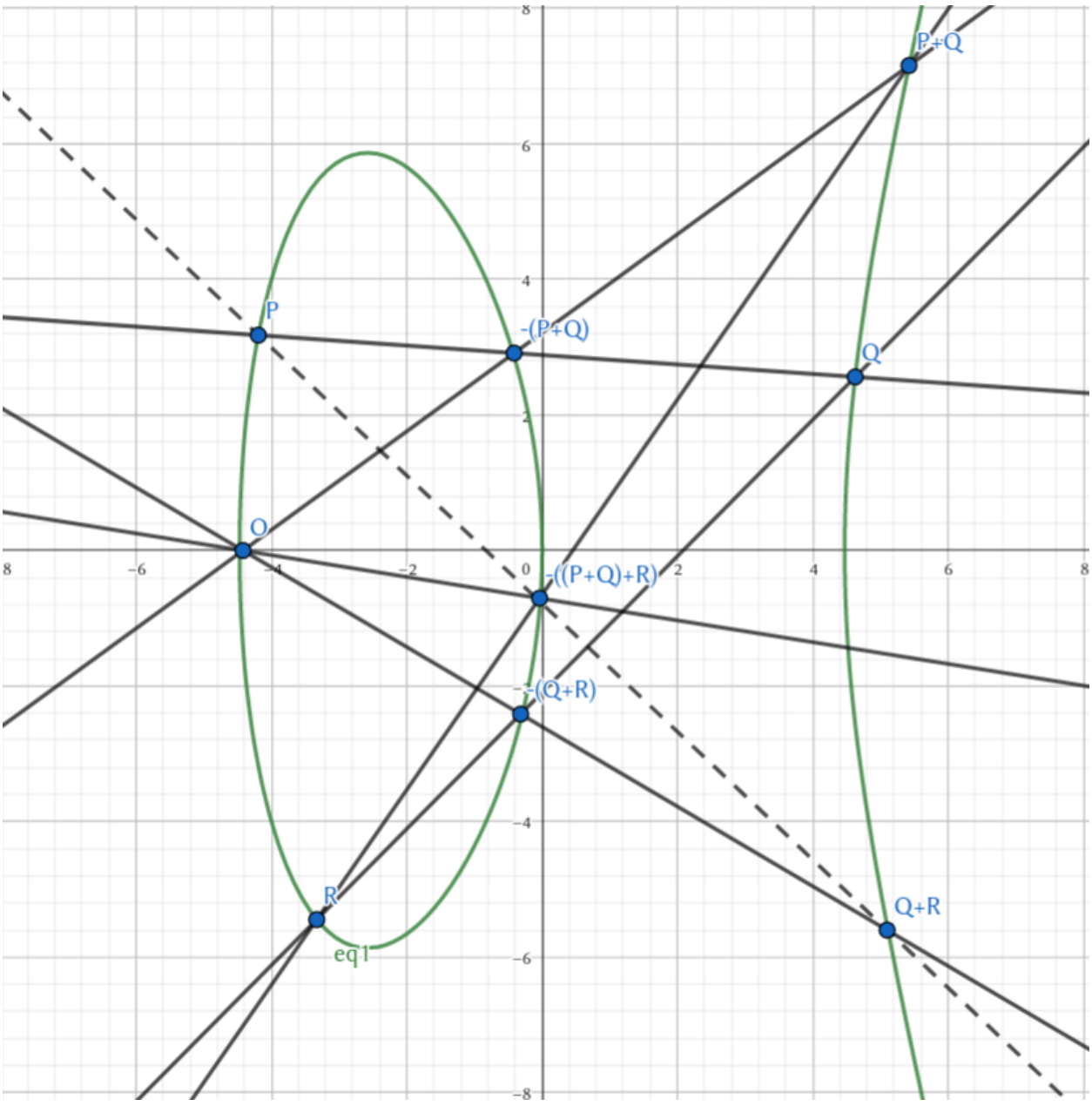


Figure 2: Adding

Rigorous definition: Consider a vector space V of maps $X \to \cup \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ Defined by

$$p \mapsto \alpha p(\alpha \in T_p^\star)$$

V is a module over $k[x]$

Any element of $k[x]$ defines a "form" in V ie. $\forall f \in k[x], df \in T_p^\star$

The space of regular diff forms $\Omega^1[X]$ on X are the elements α of V s.t. $\exists U_1, \ldots, U_n$ an open cover of X s.t. $\alpha|_{U_i} = g_1 df_1 + \cdots + g_n df_n, (g_1, \ldots, g_n, f_1, \ldots, f_n \in U_i)$ (every point $p \in X, \exists U_i$ open, finite)

Example.

$$\frac{dx}{x^3 - 1} \in \Omega^1[\mathbb{A}^1 \setminus \{\zeta_3\}]$$

on $\mathbb{A}^1$.

Also, $x^2 dx \in \Omega^1[\mathbb{A}^1]$

Maybe smoothness is needed at this point?

X affine variety	X projective variety (irr)
$k[X]$ is huge	$k[X]$ small, namely $k[X] = k$
$\Omega^1[X]$ huge	$\Omega^1[X]$ small (finite dim v.s.)

Example. $\mathbb{P}^1 = A^1 \cup A^1 k$ *where the first set is* $[\frac{x}{y} : 1]$ *and the second is* $[1 : \frac{y}{x}]$.

A regular function is $P(t)/Q(t)$. *Regular in* A^1 *is just a polynomial. Regular in* A^1 *is a polynomial in* $t^{-1} \implies$ *the polynomials are constant* $(P(t) = Q(E^{-1}) \implies P = Q \in k$

Then to compute the group of differential forms:

$\Omega[\mathbb{P}']$

$$P(t)dt = G(t)d\left(\frac{1}{t}\right) = \frac{Q(t)dt}{t^2} \implies \Omega[\mathbb{P}'] = 0. \qquad \text{(no constant works)}$$

Let E be an elliptic curve

Claim 3.1.

$$\Omega^1[E] = k$$

Notice that $\omega = dx/y$ is a form regular at $E - (\{z = 0 \cup \{y = 0\})$. By definition, we have $2ydy = (3x^2 + a)\,dx \implies \frac{dx}{y} = \frac{2dy}{3x^2+a} \in k[x]$ $\{y = 0\} \cap \{3x^2 + a\} = \varphi$ has no problems when $y = 0$.

$$\{y = c\} \cap \left\{x^2 + a\right\} = \emptyset \text{ because } (x, y) \in E.$$

Now to find identities:

$$(x_1,, y_1)\,(u, v) \in E \quad (x_1, y_1) + (u, v) = (x_2, y_2) \tag{1}$$

$$E \to_{+(u,v)} B \to \Omega^1[E] \to \Omega^1[E] \tag{2}$$

$$\frac{dx_1}{y_1} = \frac{dx_2}{y_2}$$

$\omega \longmapsto f(x, y)i$

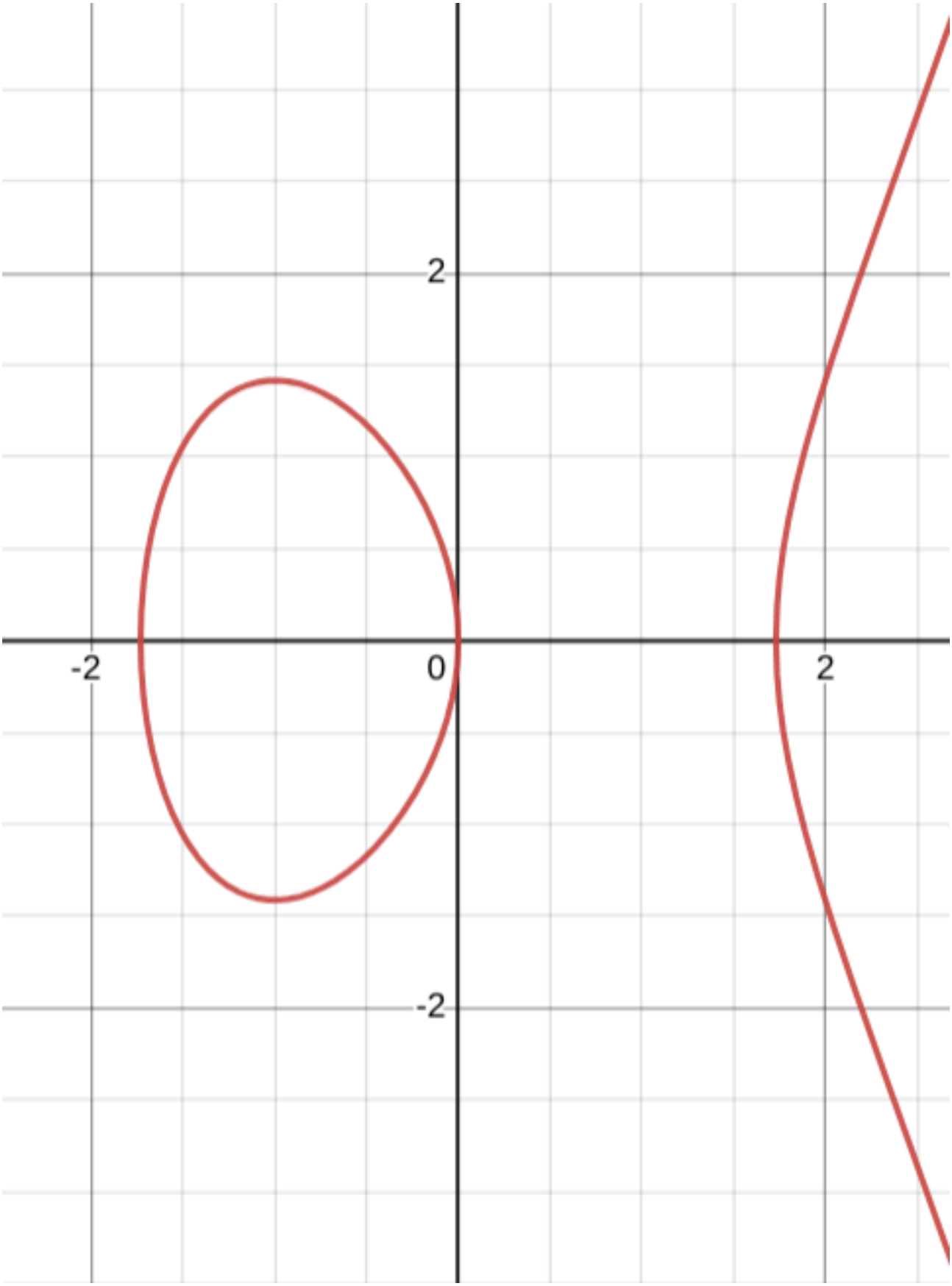


Figure 3: Some $y^2 = x^3 + ax + b$

Definition 3.3. *For X smooth projectic curve,* $\dim \Omega[x] = g$

For example, $g(\mathbb{P}) = 0 \quad g(E) = 1$.

Theorem 3.3. $k = \mathbb{C}$

Smooth projective curve $\subseteq \mathbb{P}^n_{\mathbb{C}}$ $X \subseteq \mathbb{P}^n_{\mathbb{R}}$ component wise (this is orientable)

Claim 3.2. *All surfaces are homeo to a multi-holed torus where g is num of holes*

Proof. Make a lattice Λ

$$\begin{aligned} \mathbb{C}/\Lambda &\simeq E \\ z &\longrightarrow (p(z), p'(z)), p \text{ Weierstrass function} \\ dz &\longrightarrow \frac{dx}{y} \end{aligned}$$

□