

Borcherd Algebraic Geometry 1

Rindra Razafy, “Hagamena”

September 8, 2022

Contents

0 Prologue	4
Lecture: 1 Preliminaries	5
1 Introduction	5
1.1 Examples	5
1.1.1 Pythagorean triangles	5
2 Two cubic curves	6
3 Bézout, Pappus, Pascal	7
3.1 Bézout’s theorem	7
3.2 Pappus’ theorem	7
3.3 Pascal’s theorem	7
4 Kakeya sets	8
Lecture: 2 Affine varieties	9
5 Affine space and Zariski topology	9
5.1 Affine space	9
5.1.1 Affine geometry	9
5.2 Zariski topology	10
6 Noetherian spaces and Noetherian Rings	11
6.1 Noetherian rings	11
6.2 Noetherian spaces	11
6.3 A first definition of Algebraic Varieties	12
6.3.1 Irreducible sets	12
6.3.2 Examples	12
7 Hilbert’s Nullstellensatz	13
7.1 Weak Nullstellensatz	14
7.2 Strong Nullstellensatz	14
8 The Lasker Noether Theorem	15
8.1 Some background	15
9 Quotients of varieties by groups	17
9.1 Coordinate rings	17
9.2 Application	17
9.3 Hilbert’s fintiness theorem	18
10 Three examples of quotients of algebraic sets	19
10.1 Cyclic quotient singularity	19
10.2 Parameter space of cyclohexane	20
10.3 Moduli space	20

11 Dimension	21
11.1 Definitions of Dimension	21
11.2 Algebraic definition of dimension	21
Lecture: 3 Onwards, to Projective varieties!	23
12 Projective varieties	23
12.1 Projective space over the reals	23
12.2 Projective space over complex numbers	23
12.3 Background of Projective geometry	23
12.3.1 Synthetic approach to projective geometry	24
12.3.2 Desargues' theorem	24
12.4 Duality for projective space	25
13 Affine and projective varieties	25
13.1 Examples	25
13.1.1 Twisted Cubic	26
14 Product of varieties	27
14.1 Product of projective space	27
14.2 Example of the Segre map	28
15 Two examples of Projective Varieties	28
15.1 Veronese surface	28
15.2 Variety of all lines in \mathbb{P}^3	28
15.2.1 Find cohomology of quadric in \mathbb{P}^5	29
16 Grassmannians	29
16.1 Plucker relations:	30
16.2 Applications	30
16.3 Why is the mapping natural?	31
17 More examples of projective varieties: Projective space bundles	31
17.1 Hirzebruch surfaces	31
17.2 Scrolls	32
17.2.1 Abstract varieties (Weil)	32
17.3 Toric varieties	32
17.3.1 2 dimensional example	32
Lecture: 4 Morphisms	36
18 Category Theory	36
18.1 Examples	36
18.2 Varieties and Categories	37
18.2.1 Regular functions	37
18.2.2 Regular functions on quasi-projective variety	38
18.2.3 Morphisms of varieties	38
19 Affine algebraic sets and commutative rings	39
19.1 Automorphism of space	43
20 The Ax Grothendieck theorem	44
Lecture: 5 Rational maps	46
21 Rational functions and rational maps	46
21.1 Rational maps between varieties	46
22 Elliptic functions and cubic curves	47
23 Rationality of cubic surfaces	49

24 Blowing up a point	49
24.1 Application of Blow up: Resolving singularities	50
24.1.1 Higher dimensions:	51
24.2 More on blow ups	52
25 The Atiyah flop	53
Lecture: 6 Non-singular varieties	55
26 Singular Points	55
26.1 Zariski tangent space	56
27 Du Val singularites	58
28 Resolution of singularites	60
29 Completions of a ring	62
29.1 Hensel's lemma	64
30 Elimination theory	65
Lecture: 7 Nonsingular curves	67
31 Informal review of classification of algebraic curves	67
32 Hurwitz curves	69
32.1 Example of Hurwitz curves	71
33 Desingularising an algebraic curve	72
33.1 Newton's rotating ruler	73
Lecture: 8 Intersections	76
34 Hilbert Polynomials of graded modules over a graded ring	76
34.1 Application: Degree of a variety	77
35 Bézout's theorem	78

0 Prologue

Some quick notes summarising the “Algebraic geometry 1” video lectures from R.E. Borcherds, found here.

Lecture 1: Preliminaries

1 Introduction

1.1 Examples

1.1.1 Pythagorean triangles

Problem: How do we classify all Pythagorean triangles.

We will look at two ways of solving this:

1. **Algebraic way:** We want to solve

$$x^2 + y^2 = z^2 \text{ with } x, y, z \text{ coprime integers} \quad (1)$$

If we look at the equation mod 4 we notice that $x^2, y^2, z^2 \equiv 0, 1 \pmod{4}$, since the squares mod 4 all take these forms.

So z is odd and WLOG we assume that x is even and y is odd. We rearrange the equation:

$$y^2 = z^2 - x^2 = (z-x)(z+x) \quad (2)$$

Assume that $z-x = dm_1$ and $z+x = dm_2$, therefore we have that $2z = d(m_1 + m_2)$ and $2x = d(m_2 - m_1)$, then since $d | 2z$ and $d | 2x$, and $\gcd(x, z) = 1$ we have two cases, either d divides both x and z , which would imply that $d = 1$.

Or d divides 2 which means that $d = 1$, or $d = 2$. But note that since x, z are of opposite parity $z+x$ is odd so $d \neq 2$.

So in all cases, $d = 1$. So $(z-x)$ and $(z+x)$ are coprime.

But since their product is a square this implies that $z-x$ and $z+x$ are squares, so:

$$z-x = r^2, \text{ and } z+x = s^2, \text{ where } s, r \text{ are odd and coprime} \quad (3)$$

So we conclude that $z = \frac{r^2+s^2}{2}$, $x = \frac{s^2-r^2}{2}$, $y = rs$ for any r, s odd and coprime.

2. **Geometric solution** Let $X = \frac{x}{z}$, $Y = \frac{y}{z}$ and we want to solve

$$X^2 + Y^2 = 1, \quad X, Y \text{ rational} \quad (4)$$

So we are looking for rational points on the unit circle.

Note if we draw the line from $(-1, 0)$ to (X, Y) on the unit circle with $X, T \in \mathbb{Q}$. It will intersect the y -axis at the point $(0, t)$ where $t = \frac{Y}{X+1} \in \mathbb{Q}$.

Conversely, if we are given t we can find (X, Y) , since we know that

$$Y = t(X+1) \text{ and } t^2(X+1)^2 + X^2 = 1 \Rightarrow (X+1)((t^2+1)X + t^2 - 1) = 0$$

And finding roots we see that $X = \frac{1-t^2}{1+t^2}$ and $Y = \frac{2t}{1+t^2}$, for $t \in \mathbb{Q}$.

So there is a correspondence between points on the circle except for the point at $(-1, 0)$ and points on the y -axis. This is what is called a Birational Equivalence.

Definition 1.1. Birational Equivalence An equivalence excepts on subsets of co-dimension at least 1.

Treating this problem as a geometrical problem gives us additional insights. Indeed, for example the circle forms a group of rotations with operation:

$$(x_1, y_1) \times (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \quad (5)$$

This is the cosine and sign of the sum of two angles, indeed if $(x_1, y_1) = (\cos \theta_1, \sin \theta_1)$ and $(x_2, y_2) = (\cos \theta_2, \sin \theta_2)$ then:

$$(\cos \theta_1, \sin \theta_1) \times (\cos \theta_2, \sin \theta_2) = (\cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2, \dots) = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)) \quad (6)$$

This is the simplest example of what is called an Algebraic group.

Definition 1.2. Algebraic Groups We can think of this as functor from (commutative) Rings to Groups.

$$G: R \rightarrow (\{(x, y) \in R^2 \mid x^2 + y^2 = 1\}, \times) \quad (7)$$

Where the operation is defined as above, and the identity is $(1, 0)$ and $(x, y)^{-1} = (x, -y)$.

Example 1.2.1. $G(\mathbb{C}) = \{(x, y) \in \mathbb{C} \mid x^2 + y^2 = 1\}$

But note that $1 = x^2 + y^2 = \underbrace{(x+iy)}_z \underbrace{(x-iy)}_{\bar{z}}$. So we see that

$$G(\mathbb{C}) = \{(x, y) \in \mathbb{C} \mid x^2 + y^2 = 1\} \simeq \{z \in \mathbb{C} \mid z \text{ is invertible}\} = \mathbb{C}^* \quad (8)$$

Summary There are many ways to view a circle:

1. Subset of \mathbb{R}^2
2. Polynomial $x^2 + y^2 - 1 \rightarrow$ Algebraic set
3. Ideal $(x^2 + y^2 - 1)$ in ring $\mathbb{R}[x, y]$.
4. Ring $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ = coordinate ring of S^1 . Can be seen as the set of polynomials on the circle.
5. (Smooth) manifold
6. Group (Algebraic Group)
7. Functor from Rings to Groups or Sets (Grothendieck)

2 Two cubic curves

In this section we will discuss some cubic curves.

1. $y^2 = x^3 + x^2$

There is almost a 1-to-1 correspondence between (x, y) rational on this curve and $t \in \mathbb{Q}$, via $t = \frac{y}{x}$, the slope of the line through (x, y) and the origin. Indeed since $y = tx$, if $x \neq 0$, we have:

$$t^2 x^2 = x^3 + x^2 \Rightarrow t^2 = 1 + x \Rightarrow x = t^2 - 1 \text{ and } y = t^3 - t \quad (1)$$

We don't quite get a 1-1 correspondence because $t = 1$ and $t = -1$ both correspond to $(x, y) = (0, 0)$.

So we can think of this cubic curve as a copy of \mathbb{Q} , but two of these points are mapped to the same point.

Definition 2.1. Resolution of Singularity A singularity is a “bad” point of our curve, and a resolution is getting a “nice” map from a curve without singularities to our curve.

The resolution in the above case is done by a process called “blowing-up”.

Remark. Hironaka, showed that blowing-up resolves singularites in zero characteristic. (The problem in non-zero characteristic is still unsolved).

Remark. Finding rational points on curves can be difficult. For example:

$$x^n + y^n = 1 \Rightarrow X^n + Y^n = Z^n \text{ where } x = X/Z \text{ and } y = Y/Z \quad (2)$$

This is Fermat's Last Theorem, which was very hard to solve.

2. $x^3 + y^3 = 9$

Note on this curve we can define an algebraic operation “+”, if we add in a point at infinity. In that case, the point at infinity is the identity “0”, and a, b, c on the curve lie on a line if and only if $a + b + c = 0$ in the group. To check that the group operation is associative we use the fact that: $a_1 + a_2 + \dots = b_1 + b_2 + \dots \iff$ there is a rational function with poles at a_i and zeroes at the b_i .

Definition 2.2. Groups of this kind are called **elliptic curves**, there are the 1-dimensional case of what is called **Abelian varieties**. Abelian varieties are algebraic groups that are “projective”, roughly they have no missing points.

3 Bézout, Pappus, Pascal

3.1 Bézout's theorem

Theorem 1. *Bézout* Informally: Two curves of degree m, n in the plane have at most mn intersection, if they have no components in common.

Stronger version of Bézout There have exactly mn intersection points if:

1. We are working over \mathbb{C}
2. Count points at infinity
3. Counting multiplicities (for example a straight line tangent to a parabola, we need to count the intersection point as two points).

This theorem was originally stated by Newton, though he didn't really prove it.

It is actually quite difficult to make sense of multiplicities.

Proof. Informal proof: Suppose the curves are $f(x, y) = 0$ of degree m and $g(x, y) = 0$ of degree n .

Perturb f, g so that $f = p_1 \dots p_m$ and $g = q_1 \dots q_n$, with p_i, q_j linear.

Problem: How do we know the number of intersection points doesn't change as we perturb f, g □

This style of proof was very common in the Italian School of Algebraic Geometry, but with these informal reasonings caused them to introduce many false theorems.

Weil and Zariski put Algebraic Geometry on much firmer foundations, but the proofs became much more complicated.

Nowadays, these informal proofs are mostly useful just to guess what the right answer is (for example understanding the reasoning for the above proof, we can understand the reasoning for the analogue of Bézout's theorem in higher dimensions).

3.2 Pappus' theorem

Theorem 2. Informally: Take two straight lines in the plane and on each line choose any three points. Number them and join them to every point of a different number on the other line, looking at the intersection point of these lines. These three intersection points lie on a straight line.

This theorem is equivalent to commutativity in multiplication. If we look at the analogous result in a plane over a division ring then:

Pappus' theorem is true \iff The division ring is a field (so multiplication commutes)

3.3 Pascal's theorem

Theorem 3. Informally: Choose any six points on an ellipse, separate your ellipse into two, so that three points lie on one side and three points lie on the other side. Number the points on the first side as 1,2,3 and likewise for the points on the other side. Then join them to every point of a different number on the opposite side, looking at the intersection point of these lines. These three intersection points lie on a straight line.

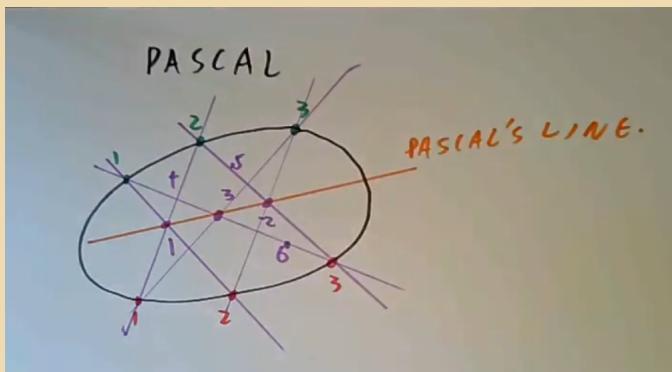


Illustration from the lecture video

The line on which their intersection lies is called the **Pascal line**.

Pappus' theorem is a degenerate case of Pascal's theorem, Pascal's theorem holds for any degree two curve and two straight lines are a degenerate case of a degree 2 curve.

How do we prove Pascal's theorem? We will use a proof using Algebraic Geometry and Bézout's theorem.

Proof. We number the lines as in the picture above (noting that they form a funny kind of hexagon) and choose six linear polynomials, p_i , for $i \in \{1, \dots, 6\}$ where $p_i = 0$ on line i .

Now look at $p_1 p_3 p_5$ and $p_2 p_4 p_6$, these polynomials vanish on all six points, so choose λ such that:

$$p_1 p_3 p_5 - \lambda p_2 p_4 p_6 \text{ this is of degree 3 curve} \quad (1)$$

Vanishes on a seventh point of the conic. Since the conic is of degree 2, by Bézout there are at most 6 intersection points UNLESS they have a common component. So the conic must be contained in the degree 3 curve.

So this degree 3 curve is equal to the union of a conic and a line, which is Pascal's line. Indeed since $p_1 p_3 p_5$ and $p_2 p_4 p_6$ both vanish on the three intersection points, since they are on the curve but not on the conic, they must be on the line. \square

4 Kakeya sets

We will continue to look at examples from Algebraic Geometry. Kakeya Sets are constructs from real analysis.

Definition 4.1. The first definition of a **Kakeya set** is a set such that if you have a unit line in the set we can turn the line around in the set, for e.g. A circle, or an equilateral triangle.

Slight variation of the definition, is that it is a set containing a unit line in every direction.

A Kakeya set over a finite field F is a set that contains a line in every direction. A conjecture from T.Wolff:

The size of a Kakeya set over F in F^n is at least $c_n |F|^n$.

This was proved in 2008 by Dvir with $c_n = \frac{1}{n!}$.

The proof is in two steps:

1. A Kakeya Set in F^n cannot lie in a hypersurface of degree $d < |F|$.

Proof. Suppose f is a polynomial of degree $d < |F|$ defining a hypersurface which is a Kakeya Set, and let f_d be the highest degree component. Note that for any v we can find x so that $f(x + vt)$ vanishes for all t . This is what is meant by the zeroes of f are a Kakeya set. For any direction v we can find a line such that f vanishes on that line.

So coefficient $f_d(v)$ of t^d vanishes for any v , so f_d has degree $< |F|$, since if f_d was non-zero it would have at most $< |F|$ zeroes we must have that $f_d = 0$. So $f = 0$. \square

2. Observe, the polynomials of degree at most $|F| - 1$ form a vector space of dimension $\binom{n+|F|-1}{n}$.

So we can find hypersurface of degree at most $|F| - 1$ vanishing on any set with less than $\binom{n+|F|-1}{n}$ points.

So a Kakeya set has at least $\binom{n+|F|-1}{n}$ points, but

$$\binom{n+|F|-1}{n} = \frac{|F|(|F|+1)\cdots(|F|+n-1)}{1\cdot 2\cdots n} \geq \frac{|F|^n}{n!}$$

Example 4.1.1. 27 lines on a cubic surface.

We will prove that the cubic surface:

$$w^3 + x^3 + y^3 + z^3 = 0 \text{ in } \mathbb{P}^3$$

Has exactly 27 lines on it.

Note $(w: x: y: z) \in \mathbb{P}^3$ then $(w: x: y: z) = (\lambda w: \lambda x: \lambda y: \lambda z)$, for all $\lambda \neq 0$.

Note there is an obvious line:

$$(a: -a: b: -b) \text{ since } a^3 + (-a)^3 + b^3 + (-b)^3 = 0$$

Note we can permute the coordinates and we can multiply by ω such that $\omega^3 = 1$.

This gives us $3 \times 3 \times 3 = 27$ possibilities.

Lecture 2: Affine varieties

5 Affine space and Zariski topology

5.1 Affine space

Definition 5.1. Let k be any field (most commonly taken as \mathbb{C} , \mathbb{R} or a finite field), then an **Affine space** is just k^n as a vector space, with slightly different automorphism group.

- automorphism of a vector space is:

$$GL_n(k) = \{n \times n \text{ matrices such that } \det \neq 0\}$$

- automorphism of Affine space is:

$$GL_n(k) \text{ and } \{\text{translations, i.e a map } x \rightarrow x + v \text{ for some vector } v\}$$

If $n = 2$ the group can be pictured of as the group of matrices of the following shape:

$$\begin{bmatrix} *_1 & *_1 & *_2 \\ *_1 & *_1 & *_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Where $\begin{bmatrix} *_1 & *_1 \\ *_1 & *_1 \end{bmatrix} \in GL_n(k)$ and $\begin{bmatrix} *_2 \\ *_2 \end{bmatrix}$ corresponds to a translation.

We write an affine space as \mathbb{A}^n .

Roughly speaking an affine space is a vector space where we have “forgotten” what our origin is.

If we have a vector space we can get an affine space by “forgetting” 0, and if we have an affine space we can choose any point to be the origin and it gives us a vector space.

Example 5.1.1. Note that if we look at the universe, the 3D space we live in is an affine space as there is no natural way to choose the origin. But if we choose the origin to be the center of the earth then 3D space becomes a vector space.

5.1.1 Affine geometry

Definition 5.2. **Affine geometry** can be thought as the study of affine space that is invariant under translations and linear transformations.

Properties of affine geometry

- points
- lines
- parallel lines
- conics
- Polynomial functions

Are all well-defined in affine geometry.

Not affine geometry

- circles
- angles
- lengths

Coordinate ring of \mathbb{A}^n Algebraic geometry tends to use the coordinate ring of affine space.

Definition 5.3. The coordinate ring of \mathbb{A}^n , is just the space of polynomials on \mathbb{A}^n . Where k is infinite. If we got affine space we can reconstruct the ring of polynomials on it. Conversely if we are given a polynomial ring over k we can reconstruct affine space as:

$$\mathbb{A}^n = \{\text{homomorphism from } k[x_1, \dots, x_n] \rightarrow k \text{ (as a } k\text{-algebra)}\}$$

Indeed a homomorphism taking $k[x_1, \dots, x_n] \rightarrow k$, just takes $x_i \rightarrow a_i$ for some $a_i \in k$. This corresponds to the point $(a_1, \dots, a_n) \in \mathbb{A}^n$.

Because of this the study of affine space is more or less equivalent to the study of this polynomial ring. In particular the automorphism group of these two are the same.

5.2 Zariski topology

Definition 5.4. An **algebraic set** is a set of zeros of some set of polynomials in $k[x_1, \dots, x_n]$.

Example 5.4.1. If $f(x, y) = x^2 + y^2 - 1$, then our algebraic set is the circle.

Example 5.4.2. If $f(x) = x - a$ and $g(y) = y - b$, the our algebraic set is the point (a, b) .

Algebraic sets are closed under these operations:

- Intersection: Indeed if C_1, C_2, \dots are the zero sets of P_1, P_2, \dots then $\bigcap C_i$ are the zeroes of $\bigcup P_i$.
- Finite unions: If C_1, C_2 are the zeroes of $\{f_1, f_2, \dots\}$ and $\{g_1, \dots\}$ respectively, then $C_1 \cup C_2$ are the zeroes of $\{f_1 g_j\}$.
- Clear that \mathbb{A}^n and \emptyset are algebraic sets, taking the zero set of 0 and of a constant non-zero polynomial respectively.

With these properties we see that we can create a topology where the closed sets are the algebraic sets. We call this topology the **Zariski topology**.

Example 5.4.3. Take \mathbb{A}^1 , this is just the line. The closed sets:

- \mathbb{A}^1 , the zero set of 0.
- Any finite sets, since $\{a_1, \dots, a_n\}$ is the zero set of $(x - a_1) \cdots (x - a_n)$

These are the only closed sets, since a polynomial in one variable is either the zero polynomial or has a finite amount of roots.

Take any points $x \neq y$ and nbhs U of x and V of y . Since U^c and V^c are finite (note if they are infinite then U or V is the empty set which is impossible). So U and V both contain all the points of \mathbb{A}^1 except for a finite number of points. Since k is infinite this means that $U \cap V \neq \emptyset$. This is true for all nbhs of x and y , which means this space is not Haussdorff.

Example 5.4.4. Take \mathbb{A}^2 . The closed sets are:

- Points (a, b)
- Any curve, the set of zero of $f(x, y) = 0$
- Union of finite amount of curves and points

Note $\mathbb{A}^2 \neq \mathbb{A}^1 \times \mathbb{A}^1$. Indeed since $\mathbb{A}^1 \times \mathbb{A}^1$ are unions of finite amount of vertical lines, horizontal lines and points.

Example 5.4.5. Determinantal variety: Take $\mathbb{A}^{mn} = \text{linear maps } k^m \rightarrow k^n = m \times n \text{ matrices}$

Determinantal variety = set all linear maps of rank $\leq i$.

We claim that this is an algebraic set. Indeed this set is given by the vanishing of all $(i+1) \times (i+1)$ minors of $m \times n$ matrix. This is a set of polynomials.

In particular the subset of maps from $k^m \rightarrow k^n$ that are onto is open in the Zariski topology.

6 Noetherian spaces and Noetherian Rings

6.1 Noetherian rings

Definition 6.1. A **Noetherian ring** is a ring satisfying these three equivalent conditions:

- Every ideal is finitely generated
- Every nonempty set of ideals has a maximal element
- Every chain of increasing ideals, $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$, is eventually constant. I.e. there is a n such that $I_n = I_m$ for all $m \geq n$.

Theorem 4. Noether

If R is Noetherian then $R[x]$ is Noetherian.

Proof. Let I be an ideal of $R[x]$ and look at the chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$, of R where:

$$I_n = \text{leading coeffs of polynomials of degree } \leq n \text{ in } I$$

Since R is Noetherian this stabilises, so $I_N = I_{N+1} = \dots$, for some N .

Take the set of polynomials s_0, s_1, \dots, s_N where:

$$s_i = \text{degree } i \text{ polynomials whose leading coefficients generate } I_i, \text{ for } i = 1, \dots, N$$

Note the sets s_i are finite since R is Noetherian.

Then s_0, s_1, \dots, s_N generate the ideal I . □

Corollary 4.1. Hilbert

$k[x_1, \dots, x_n]$ is Noetherian

Proof. Since k is a field any ideal in k is either generated by 0 or generated by 1. So k is Noetherian, so $k[x_1]$ is Noetherian. So inductively we can see that $k[x_1, \dots, x_n]$ is Noetherian. □

6.2 Noetherian spaces

Definition 6.2. A topological space is called **Noetherian** if equivalently:

- The closed sets satisfy the descending chain condition. So any decreasing sequence:

$$C_0 \supseteq C_1 \supseteq C_2 \supseteq \dots$$

Stabilises, i.e. $C_n = C_{n+1} = \dots$, for some n

- Any nonempty collection of closed sets has a minimal element.

These are in some sense the dual of the definition of Noetherian Ring.

Theorem 5. \mathbb{A}^n with Zariski topology is Noetherian.

Proof. Sketch:

Closed sets of \mathbb{A}^n correspond to some ideals of $k[x_1, \dots, x_n]$. A descending chains of closed sets of \mathbb{A}^n correspond to an ascending chain of ideals in $k[x_1, \dots, x_n]$. □

Noetherian spaces are “WEIRD”, the Noetherian condition is equivalent to saying that every open set is compact or quasicompact. Note quasicompact actually means the same as the regular defintion of compact, Bourbaki made a mistake in the defintion and only considered Haussdorff compact spaces to be compact, so when non-Haussdorff compact spaces were seen to be important they had to use the term quasicompact.

Borcherds' Rule of Thumb If we see the word “quasi” in mathematics then someone, somewhere and somehow screwed up the terminology and had to use the term “quasi” to fix it.

Remark. In analysis we almost never see open compact sets, it can be shown that if a space is Noetherian and Haussdorff then it is finite.

6.3 A first definition of Algebraic Varieties

6.3.1 Irreducible sets

Definition 6.3. A set is called **irreducible** if and only if it is nonempty and not the union of 2 proper closed subsets.

Definition 6.4. Noetherian Induction, pick a maximal closed set of some collection of closed sets.

Theorem 6. Any Noetherian space is a finite union of irreducible subspaces.

Proof. Proof by Noetherian Induction:

We will show that every closed subset is a finite union of irreducibles. If not, pick a minimal counterexample C . We have two cases

1. If C is irreducible, then we are done and we have found a contradiction
2. If C is not irreducible, then we can write $C = C_1 \cup C_2$, where C_1, C_2 are smaller. By induction, C_1, C_2 are a finite union of irreducible sets, and so is C . Which is a contradiction.

In all cases we have a contradiction so, there can't be a closed set that is not a finite union of irreducibles. So all closed sets, in particular the whole space is a finite union of irreducibles. \square

So we can reduce the study of Noetherian spaces to the study of irreducible Noetherian spaces.

Corollary 6.1. Every algebraic set is a finite union of irreducible algebraic sets.

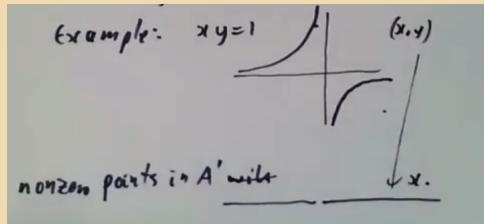
Definition 6.5. A provisional definition of Algebraic Varieties:

They are irreducible closed subset of affine space.

6.3.2 Examples

Example 6.5.1. This definition is not perfect. Suppose we take the variety given by: $xy = 1$ and the set of nonzero points in \mathbb{A}^1 .

Note the set of nonzero points in \mathbb{A}^1 is not a closed set, but since we can map the hyperbola to this by the mapping $(x, y) \rightarrow x$, we should consider it an algebraic variety.



We shall give a better definition later (I guess we can look at these like “quasi-algebraic varieties”).

Example 6.5.2. Take the algebraic set defined by $x^2 + y^2 - 2z^2 = 0$ and $2x^2 - y^2 - z^2 = 0$.

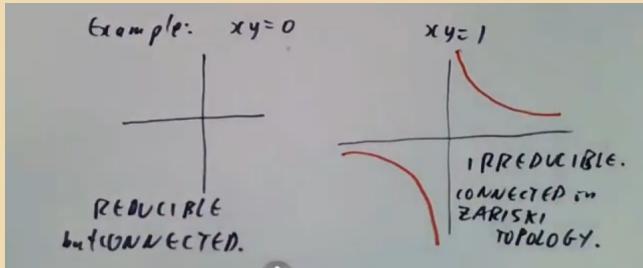
This is the union of four irreducible subsets:

1. $x = y = z$
2. $x = 0, y = z$
3. $x = -y = -z$
4. $x = y = -z$

So the intersection of irreducible sets may not be irreducible.

Example 6.5.3. If we take $xy = 0$, we have the union of the x -axis and the y -axis.

If we take $xy = 1$, we have a hyperbola, which is irreducible and connected in the Zariski topology, but disconnected in the usual topology.



We have now concluded the section on Noetherian spaces, next section we will look at the Hilbert Nullstellensatz, and the connection between Algebraic Varieties and Ideals.

7 Hilbert's Nullstellensatz

Definition 7.1. Hilbert's Nullstellensatz(zero's theorem) describes the relation between Ideals in a polynomial ring and Algebraic subsets of the corresponding affine sets.

- If we have a subset $Y \subseteq \mathbb{A}^n$ we can map it to the ideal $I(Y) \subseteq k[x_1, \dots, x_n]$ where $I(Y)$ is the set of polynomials vanishing on Y .
- If we have an ideal $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ we can map it to the set $Z(\mathfrak{a})$ which is the set of zeros of all the polynomials of \mathfrak{a} .

What is the relationship between these two operations?

$$Z(I(Y)) = \text{closure of } Y \text{ in the Zariski topology}$$

This fact basically comes from the definition of the Zariski topology, let W be any closed set containing Y . We know that W is the zero set of some set of polynomials S . For all $f \in S$ we have:

$$f(x) = 0 \text{ for all } x \in Y$$

Therefore $S \subseteq I(Y)$, therefore for all $f \in S$ and we have by definition of $Z(\cdot)$:

$$f(y) = 0 \text{ for all } y \in Z(I(Y))$$

So $y \in Z(S)$, therefore $Z(I(Y)) \subseteq W = Z(S)$. Since $Z(I(Y))$ is the smallest closed set containing Y we indeed see that it is the closure.

On the other hand is it true that $I(Z(\mathfrak{a})) = \mathfrak{a}$ for all ideal $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$? **NO**:

Example 7.1.1. Let $\mathfrak{a} = (x^2) \subseteq k[x]$, and $Z(\mathfrak{a}) = 0$ so $I(Z(\mathfrak{a})) = I(0) = (x)$.

More generally, if $f^n \in \mathfrak{a}$, then $f \in I(Z(\mathfrak{a}))$, since certainly f vanishes at all points of $Z(\mathfrak{a})$ since f^n does. Therefore

$$\{f \in k[x_1, \dots, x_n] \mid f^n \in \mathfrak{a}, \text{ for some } n \in \mathbb{N}^*\} = \sqrt{\mathfrak{a}} \subseteq I(Z(\mathfrak{a}))$$

Note $\sqrt{\mathfrak{a}}$ is an ideal.

Is $\sqrt{\mathfrak{a}} = I(Z(\mathfrak{a}))$? **NO!**

Example 7.1.2. If $\mathfrak{a} = (x^2 + 1) \in \mathbb{R}[x]$, then $Z(\mathfrak{a}) = \emptyset$, and $I(Z(\mathfrak{a})) = \mathbb{R}[x] \neq \sqrt{(x^2 + 1)} = (x^2 + 1)$

7.1 Weak Nullstellensatz

What are the maximal ideals of a polynomial ring $k[x_1, \dots, x_n]$? There are Obvious maximal ideals:

Let $(a_1, \dots, a_n) \in \mathbb{A}^n$ and take the ideal $(x - a_1, x - a_2, \dots, x - a_n)$ =functions vanishing on (a_1, \dots, a_n) .

Note that

$$k[x_1, \dots, x_n]/(x - a_1, x - a_2, \dots, x - a_n) \simeq k$$

So this is a maximal ideal. Are all ideals of this form? Not in general, if we take $\mathbb{R}[x]$ then $(x^2 + 1)$ is a maximal ideal, since $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

But this is true if k is **Algebraically closed!** This is the weak Nullstellensatz.

Theorem 7. Weak Nullstellensatz For k algebraically closed all maximal ideals of $k[x_1, \dots, x_n]$ are of the form $(x_1 - a_1, \dots, x_n - a_n)$.

Proof.

Lemma 8. If K is a field an is a finitely generated algebra over k , then K is a finitely generated module over k .

Proof. We are going to cheat: We will assume that k is uncountable. (If k is countable the proof is harder).

Since K is a finitely generated algebra, then K is at most countable dimension as a module. If $x \in K$ is transcendental over k , if we had, for some $a_1, \dots, a_n \in k$ such that $\sum_{k=1}^n \frac{a_k}{x-a_k} = 0 \Rightarrow \sum_{k=1}^n a_k \prod_{i \neq k} (x - a_i) = 0$, which is impossible since x is transcendental.

So the elements $\frac{1}{x-a}$ for $a \in k$ form an uncountable linearly independant set, which is a contradiction to the fact that K is a finitely generated algebra over k .

So all $x \in K$ are algebraic over k , therefore K is finitely generated as a module over k . \square

Suppose that I is a maximal ideal of $k[x_1, \dots, x_n]$ we want to show that $I = (x - a_1, \dots, x - a_n)$ for some (a_1, a_2, \dots) .

Let $K = k[x_1, \dots, x_n]/I$, then K is a field and is finitely generated as an algebra. So by the previous lemma K is finitely generated as a module. In other words K is algebraic over k ,

But since we assumed that k is algebraically closed we have $k = K$.

Therefore, $x_i + I \in k$ for all i so $x_i + I = a_i + I$ for some $a_i \in k$ so $x_i - a_i \in I$. So $(x_1 - a_1, \dots, x_n - a_n) \subseteq I$ so $I = (x_1 - a_1, \dots, x_n - a_n)$, since $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal and $I \neq k[x_1, \dots, x_n]$. \square

7.2 Strong Nullstellensatz

Proof of SN with Rabinovitsch trick

Theorem 9. Strong Nullstellensatz If k is algebraically closed then for all ideals $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ we have $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. Suppose that \mathfrak{a} is generated by elements f_1, \dots, f_n and that $f \in I(Z(\mathfrak{a}))$, we want to show that $f \in \sqrt{\mathfrak{a}}$.

Rabinovitsch idea is too add an extra variable x_0 .

So $f_1, \dots, f_m, 1 - x_0 f$ have no common zeroes in \mathbb{A}^{n+1} , since if x is a zero of f_1, \dots, f_n then it is a zero of f , so $1 - x_0 f(x) = 1$.

Now apply the weak Nullstellensatz in \mathbb{A}^{n+1} , since $f_1, \dots, f_m, 1 - x_0 f$ have no common zeroes, they are not contained in any of the maximal ideals(Since if they are contained in a maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$ then (a_1, \dots, a_n) would be a common zero) so they generate the unit ideal.

So there exists $g_i \in k[x_0, x_1, \dots, x_n]$ such that $1 = a_0(1 - x_0 f) + g_1 f_1 + \dots + g_n f_n$

Let $x_0 = \frac{1}{f}$, (we are now working in the ring of rational function) we have:

$$1 = g_1 \left(x_1, \dots, x_n, \frac{1}{f} \right) f_1 + g_2 \left(x_1, \dots, x_n, \frac{1}{f} \right) f_2 + \dots + g_n \left(x_1, \dots, x_n, \frac{1}{f} \right) f_n$$

We can clear denominators by multiplying by a high power of f and we get:

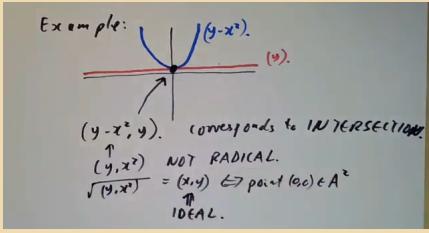
$$f^n = \sum h_i f_i \text{ where } h_i = f^n g_i \in k[x_1, \dots, x_n]$$

So $f^n \in (f_1, \dots, f_n)$ so $f \in \sqrt{(f_1, \dots, f_n)} = \sqrt{\mathfrak{a}}$. \square

Affine space \mathbb{A}^n	correspondence	$k[x_1, \dots, x_n]$
Points (a_1, \dots, a_n)	\Leftrightarrow <i>Weak Nullstellensatz</i>	maximal ideals (x_1, \dots, x_n)
Algebraic sets	\Leftrightarrow <i>Strong Nullstellensatz</i>	Radical ideals $\mathfrak{a} = \sqrt{\mathfrak{a}}$
closed subschemes	\Leftrightarrow <i>Will see in second part of course</i>	All Ideals

Example 7.1.3. In this example we have a curve described by the radical ideal $(y - x^2)$ and one given by the radical ideal (y) .

We look at the intersection between the two curves by looking at the zero set of the ideal $(y - x^2, y) = (y, x^2)$. However, this ideal is not a radical ideal, as the root of this ideal is (x, y) which corresponds to the point $(0, 0)$ in affine space.



So we have a non-radical ideal that is the intersection of two curves. This ideal is non-radical since if we look at the intersection between the two curves we should be counting the intersection point as two points.

Example 7.1.4. Nilpotent matrices

Definition 7.2. A matrix $A \in M_n(k) \simeq \mathbb{A}^{n^2}$ is **Nilpotent** if $A^n = 0$ for some $n \in \mathbb{N}$,

Notice that if:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots \\ a_{21} & & \\ \vdots & & \end{bmatrix} \Rightarrow A^n = [\text{something complicated, homogenous polynomials in degree } n \text{ in coeffs } a_{ij}]$$

The entries of the matrix A^n generate an ideal I in the coordinate ring of \mathbb{A}^{n^2} , in some sense this ideal describes the set of nilpotent matrices. Is $I = \sqrt{I}$? The answer is NO!

If A is nilpotent, then all eigenvalues are 0, so the trace is 0. So $a_{11} + a_{22} + \dots + a_{nn} \notin I$, but this element is in \sqrt{I} by Hilbert's Nullstellensatz.

Let us take $n = 1$, let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $A^2 = 0$. But $A^2 = \begin{bmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{bmatrix}$

So $I = (a^2 + bc, b(a+d), c(a+d), d^2 + bc)$. We have seen that some power of $\text{tr}(A) = a + d$ is in I . What is the smallest power? An easy assumption is that $(a + d)$ is in I , but this is false! The smallest power of $(a + d)$ in I is given for $(a + d)^3$.

$$(a + d)^2 = a^2 + 2ad + d^2$$

$$(a + d)^3 = a^3 + 3a^2d + 3ad^2 + d^3 \quad (1)$$

What about commuting matrices?

Example 7.2.1. Let $AB = BA$, with $A = (a_{ij}), B = (b_{ij}) \in M_n(k)$.

Let I be the ideal generated by the entries in $AB - BA$, is $I = \sqrt{I}$?

We don't know this is a hard open problem.

8 The Lasker Noether Theorem

8.1 Some background

Let us recall that Algebraic sets correspond to radical ideals. Since algebraic sets correspond to finite unions of irreducible algebraic sets, and these sets corresponds to Prime ideals, from this we can conclude the following theorem.

Theorem 10. Any radical ideal is the intersection of finite number of prime ideals.

Question: What about ideals that are not radical? Is there a similar decomposition? The answer is given to us by Lasker: Ideals of $k[x_1, \dots, x_n]$ is the intersection of a finite number of primary ideals.

Noether generalised this theorem by showing that it is true for Noetherian rings.

Definition 8.1. Associated Prime Let M be a module over R , and **associated prime** \mathfrak{p} is a prime ideal \mathfrak{p} such that M contains a submodule isomorphic to R/\mathfrak{p} , for brevity we write $R/\mathfrak{p} \subseteq M$.

Definition 8.2. Coprimary Module We have two definitions:

- A module M over R is called **coprimary** if:

$$ab = 0, \text{ for } a \in R \text{ and } b \in M, \Rightarrow b = 0 \text{ or } a^n = 0 \text{ for some } n \quad (\dagger)$$

- *A more convenient definition* A module M over R is coprimary if it has exactly one associated prime \mathfrak{p} .

Remark. If the ring R is Noetherian, the two definitions of coprimary are equivalent for finitely generated modules.

Definition 8.3. Primary ideal

- *A first definition by Lasker:* $\mathfrak{p} \subseteq R$ is primary if and only if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b^n \in \mathfrak{p}$ for some n .

Example 8.3.1. In $k[x]$: (x) is prime and (x^n) is primary. Note in general primary ideals need not be powers of prime ideals

- *Another definition:* An ideal $\mathfrak{p} \subseteq R$ is primary if and only if the module R/\mathfrak{p} is coprimary

Remark. In general for a module M over R , $N \subseteq M$ is primary $\iff M/N$ is coprimary.

There are two different definitions for this primary ideal under the other definition but they are equivalent if R is Noetherian.

Theorem 11. Lasker-Noether Theorem for finitely generated modules over Noetherian Rings

Let M be a f.g. module over a Noetherian Ring. Then 0 an intersection of primary submodules of M .

Alternatively: $M \subseteq \bigoplus_{\text{finite}} \text{coprimary modules}$

Example 8.3.2. For \mathbb{Z} -modules (abelian groups): Some example of coprimary modules:

- \mathbb{Z}^n where the prime ideal is (0)
- Any finite group of order p^n where the prime ideal is (p)

So our theorem says that a finitely generated abelian group is contained in direct sum of copies of \mathbb{Z} and finite groups of prime power order. If we recall the structure theorem this inclusion is actually an equality.

Proof. Lasker-Noether Theorem

This proof has two steps:

1.

Lemma 12. Any submodule M is an intersection of a finite number of irreducible submodules.

Proof. Noetherian Induction. What does this mean? The submodules of M have the property that any non-empty subset has a maximal element (since M is f.g. over a Noetherian ring). So suppose N is a maximal submodule that is not a finite intersection of irreducibles, so either this submodule is irreducible which is a contradiction since it is an intersection of itself, or it is the intersection of two larger submodules which are by induction a finite intersection of irreducibles, contradiction. \square

2.

Lemma 13. Any irreducible submodule N is primary

Proof. We can reduce to the case where N is 0 by taking quotients. So we want to show that (0) is irreducible implies that M is coprimary.

But if M is not coprimary, then there are two associated primes $\mathfrak{p}, \mathfrak{q}$ such that M has submodules isomorphic to R/\mathfrak{p} and R/\mathfrak{q} .

These submodules have intersection 0 which implies that 0 is not irreducible. \square

Combining the two previous lemmas gives us our proof. \square

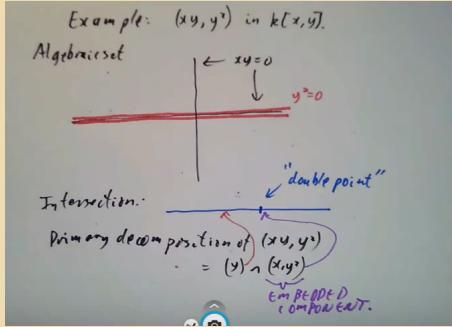
Example 8.3.3. Let us look at the ideal generated by (xy, y^2) in $k[x, y]$.

The algebraic set is given by the intersection of $V(xy) = x$ and $y - \text{axis}$ and $V(y^2) = x\text{-axis}$ (doubled up in some informal sense).

The intersection of these two sets is just the x -axis, with a sort of “double point” near the origin.

We can understand this “double point” by looking at the primary decomposition of the ideal:

$$(xy, y^2) = (y) \cap \underbrace{(x, y^2)}_{\text{embedded component}}$$



Note this primary decomposition is not unique:

$$\begin{aligned} (xy, y^2) &= (y) \cap (x, y^2) \\ &= (y) \cap (x + y, y^2) \end{aligned}$$

9 Quotients of varieties by groups

9.1 Coordinate rings

Recall for any algebraic set, Y we can go to its coordinate ring $k[x_1, \dots, x_n]/I(Y)$, this can be thought of as the ring of all polynomials on the algebraic set Y . Because we are basically “setting to zero” all the polynomials which vanish on Y , so any two polynomials that are equal on Y are considered the same. So we can find an isomorphism between the ring of polynomials on Y and this coordinate ring by sending $f + I(Y) \rightarrow f|_Y$. This is well defined since if $g + I(Y) = f + I(Y)$, then since $g - f \in I(Y)$, $g(\bar{x}) = f(\bar{x})$ for $\bar{x} \in Y \Rightarrow f|_Y = g|_Y$.

This is an injection since if $f|_Y = g|_Y$, then $g(\bar{x}) = f(\bar{x})$ for $\bar{x} \in Y$, so $f - g \in I(Y) \Rightarrow f + I(Y) = g + I(Y)$.

Finally let ω be any polynomial on Y , then $\omega(x_1, \dots, x_n) = \sum_i a_i m_i(x_1, \dots, x_n)$, for some monomial m_i . So we just need to set $f = \sum_i a_i m_i(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$.

This coordinate ring has three properties:

1. Algebraic over k
2. finitely generated
3. No nilpotent elements

On the other hand, if we have an algebra with these three properties, then by strong Nullstellensatz it corresponds to an algebraic set which is not unique, since it depends on the generators chosen. But they are isomorphic in some sense.

Informally algebraic sets (up to isomorphism) as being more or less equivalent to algebras with the above properties. In technical terms the category of algebraic sets is equiv to opposite of category of coordinate rings.

9.2 Application

Suppose we have an algebraic set Y acted on by a group G . Can we form the quotient Y/G ? This doesn't really work. One of the problems is how do we embed the quotient in affine space? But if we look at coordinate rings this is easier to do, since the functions on Y/G should correspond to the functions on Y invariant under G .

So we can look at the **Ring of invariant** $\left(k[x_1, \dots, x_n]/I(Y)\right)^G$.

So not this is an algebra over k and has no nilpotent elements, but is it finitely generated? The answer is sometimes, but Hilbert proved that in many cases it is finitely generated but some examples of when it isn't finitely generated were found after him.

Example 9.0.1. Let $\mathbb{A}^n = \text{affine space}$, and $G = S_n$ permutations of coordinates. The polynomial ring is $k[x_1, \dots, x_n]^{S_n}$ which is generated by the **elementary invariant polynomial**:

- $p_1 = x_1 + \dots + x_n$
- $p_2 = x_1 x_2 + \dots$
- \vdots
- $p_n = x_1 \dots x_n$

So

$$\mathbb{A}^n / S_n \simeq \mathbb{A}^n$$

While this example is easy, in general quotients of affine space by groups are complicated. Most of times we get a nice answer when the group is a reflection group (like S_n).

Remark. We have to be careful, the quotient might not be what we expect. If we take the real line and have the group $\mathbb{Z}/2\mathbb{Z}$ acting by $x \rightarrow -x$, we might think that the quotient is the half closed interval (which us what we would get if we were identifying points) it isn't the same as what we get in our construction above.

We get the whole real line back. The positive points are given by identifying $(2, -2)$ but the points in the negative side are given by identifying $(2i, -2i)$, these points look like complex points but they count as real points in the quotient.

Example 9.0.2. Let us look at:

$$GL_n(k) \text{ acting on } k^n \Rightarrow \text{The orbits are } 0, \text{ or everything else} \quad (1)$$

So we might think that the quotient would give us two points, but instead we only have one point since the only invariant polynomials acted on by $GL_n(k)$ are constants. Since we have for all $A \in GL_n(k)$:

$$f(A(x_1, \dots, x_n)) = f(x_1, \dots, x_n) \text{ for all } (x_1, \dots, x_n) \in k^n$$

Then pick any non-zero points $(x_1, \dots, x_n); (y_1, \dots, y_n)$ and we see that $f(x_1, \dots, x_n) = f(A(x_1, \dots, x_n)) = f(y_1, \dots, y_n)$ for some $A \in GL_n(k)$. Since this polynomial is the same at an infinite amount of points, it is the constant polynomial.

So the only invariant polynomials are the constant polynomials, this ring is isomorphic to k which is the coordinate ring of a point.

Example 9.0.3. Classical invariant theory Let $G = SL_2(\mathbb{C})$, it acts on $a_n x^n + a_{n-1} x^{n-1} y + \dots + a_0 y^n$, by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$$

So $(a_0, \dots, a_n) \in \mathbb{A}^n$ we can ask what is $\mathbb{A}^{n+1} / SL_2(\mathbb{C})$? The coordinate ring are all polynomials in (a_n, a_{n-1}, \dots) which are invariant under $SL_2(\mathbb{C})$. These are called invariants and finding them is part of classical invariant theory.

For example $a_2 x^2 + a_1 x y + a_0 y^2$, the invariant is the **discriminant** which is $a_1^2 - 4(a_0 a_2)$

Is the ring of invariants finitely generated? Paul Gordan ("king of invariant theory") proved that this was true, but Hilbert gave us an shorter way of proving this, the **Hilbert finiteness theorem**.

9.3 Hilbert's finiteness theorem

Definition 9.1. Let $A = k[x_1, \dots, x_m]$ and G be a group acting on $k^n = \text{span}\{x_1, \dots, x_m\}$ so G acts on A . Let A^G =invariant elements of A and assume that G is finite and $\text{char}k = 0$. We define the **Reynolds operator** to be ρ , where $\rho(a) =$ average of A under G . So for G finite we have

$$\rho(a) = \frac{1}{|G|} \sum_{g \in G} g(a) \quad (1)$$

Note we needed the assumptions in our statement to define this number (the sum is defined since G is finite and we can define the average since characteristic of k is zero, so we are not dividing by zero).

This operator has the following properties:

- $\rho(1) = 1$

- $\rho(a + b) = \rho(a) + \rho(b)$
- In general $\rho(ab) \neq \rho(a)\rho(b)$, this is not a homomorphism of algebras
- $\rho(ab) = a\rho(b) = \rho(a)\rho(b)$, if $a = \rho(a)$

So ρ is a homomorphism from A to A^G of A^G modules.

Theorem 14. Let $A = k[x_1, \dots, x_m]$ and G be a group acting on $k^n = \text{span}\{x_1, \dots, x_m\}$ so G acts on A . Let $A^G = \text{invariant elements of } A$. A^G is finitely generated as a k -algebra if G is finite and $\text{char } k = 0$.

Proof. Notice that A is graded by degree:

$$A = A_0 \oplus A_1 \oplus A_2 \dots \quad (2)$$

Where $A_0 = k$, $x_1, \dots, x_n \in A_1$, etc... This is the usual way of grading a polynomial ring.

Let $I = \text{ideal of } A$ generated by the homogenous elements of A^G of degree greater than zero. Notice that I is finitely generated as an ideal, we can assume that it has a finite number of generators in A^G and are homogenous.

Suppose i_1, \dots, i_n are generators as above for the ideal I , we want to show they generate the k -algebra A^G .

We show by induction of the degree that if $x \in A^G$ and x is homogenous, then x is in the algebra generated by i_1, \dots, i_n .

This is obvious for degree 0, so assume that $\deg x > 0$. Let $x = a_1 i_1 + \dots + a_k i_k$, for some $a_i \in A$ homogenous. So x is in the ideal generated by i_1, \dots, i_n but a_i NEED NOT be in A^G .

Applying the Reynolds operator:

$$x \underset{x \in A^G}{=} \rho(x) = \rho(a_1)i_1 + \rho(a_2)i_2 + \dots$$

Since $\rho(i_m) = i_m$ (since $i_m \in A^G$).

By properties of the Reynolds operator $\rho(a_i) \in A^G$, therefore x is a polynomial in elements of A^G of smaller degree. So $\deg \rho(a_i) < \deg x$ so by induction a_i are polynomials in i_m and so x is also. \square

Hilbert didn't just prove this for finite groups but also for more general groups.

Extensions of this theorem

1. For G compact and $k = \mathbb{R}$ or \mathbb{C} , the same proof works since we can define a Reynolds operator: $\rho(a) = \frac{1}{\text{vol } G} \int_G g(a)$
2. $SL_n(\mathbb{C})$? We use Weyl's unitarian trick. Since $SL_n(\mathbb{C}) \supseteq \underbrace{SU_n(\mathbb{C})}_{\text{compact}}$. Complex actions of $SL_n(\mathbb{C})$ on complex vector space V (finite dimension) are the "same" as actions of $SU_n(\mathbb{C})$ on V .

Nagata's Example This is an example of group G acting on k^n so that A^G is not finitely generated.

First take group $k \simeq \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ acts on k^2 , (this is a sort of universal counter example to everything called the **Unipotent action**, where all eigenvalues of all matrices are 1).

Then take sixteen copies of this so k^{16} acts on k^{32} , and G = "generic" 13-dim subspaces of k^{16} .

10 Three examples of quotients of algebraic sets

10.1 Cyclic quotient singularity

We take \mathbb{A}^2 whose coordinate ring is $k[x, y]$. And $G = \mathbb{Z}/n\mathbb{Z}$ generated by σ of order n , where $\sigma(x) = \zeta x$ and $\sigma(y) = \zeta y$, where ζ is a n -th root of unity.

Now what are the invariants of the coordinate ring over G ?

Well notice that

$$\sigma(x^i y^j) = \zeta^i x^i + j x^i y^j = x^i y^j \text{ if and only if } i + j = 0 \pmod{n} \quad (1)$$

So the ring of invariants has a basis $x^i y^j$, where $i + j = 0 \pmod{n}$. This ring is generated by $z_0 = x^3$, $z_1 = x^2 y$, $z_3 = x y^2$, $z_4 = y^3$, but these elements are not independent, since $z_i z_j = z_k z_l$ when $i + j = k + l$

So in reality the ring of invariant is equal to

$$k[z_0, \dots, z_4]/(z_1 z_2 = z_0 z_3, z_1^2 - z_0 z_2, z_2^2 - z_1 z_2) \quad (\dagger)$$

So the quotient of the affine plane by the cyclic group is an affine variety whose coordinate ring is the \dagger

10.2 Parameter space of cyclohexane

Definition 10.1. A **parameter space** is some sort of space whose points corresponds to some “configurations”, say some sort of algebraic subset of an algebraic variety. Like a parameter space of line inside of space, or parameter space of conics in a plane

We are going to look at the parameter space of cyclohexane, recall from chemistry cyclohexane is a ring of six carbon atoms and sixteen hydrogen atoms.

A carbon atoms centre is specified by three number so a carbon atom corresponds to \mathbb{A}^3 , so six carbon atoms correspond to $\mathbb{A}^{3 \cdot 6} = \mathbb{A}^{18}$. However there are some conditions that this need to satisfy, if one carbon atom is (x_1, y_1, z_1) and another is (x_2, y_2, z_2) they must satisfy:

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2 = c \text{ a constant} \quad (1)$$

So 6 quadrics must be satisfied for the distances and 6 for the angles. So we have 18-dimension affine space and the points must satisfy 12 equations. Subce we can translate and rotate our cyclohexane then we can guess that the parameter space is taken by:

$$\text{space of dimension } 18 - 6 - 6/\text{group of translations, rotations (six dimension group)} \quad (2)$$

What is the dimension? 0? **NO** There are two different forms of cyclohexane, the chair form and the boat form. Furthermore the boat form is felxible and we can bend it around to form another boat form.

So parameter space has at least two components, one component that is a point corresponding to the chair form and a one dimensional component corresponding to the boat form of cyclohexane.

So we must be a bit careful when guessing dimension of quotients, the naïve guess is sometimes just wrong.

10.3 Moduli space

Definition 10.2. A **moduli space** is space whose points corresponds to isomorphism classes of things

This is similar to a parameter space, it is traditional to use paramater space if we are classifying thins embedding in something else, and moduli space if we are classifying things that aren't really embedded in anything.

Now let us look very briefly at the moduli space of elliptic curves.

Definition 10.3. A **Elliptic curve** over the complex numbers is a non-singular curve that is topologically isomorphic to a torus. (We will discuss elliptic cutves lates)

We will later see that elliptic curves can be written as:

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c \\ y^2 &= (x - \alpha)(x - \beta)(x - \gamma) \\ y^2 &= x(x - \beta)(x - \gamma) \text{ by adding a constant to } x \\ y^2 &= x(x - 1)(x - \lambda) \text{ by rescaling } x, \text{ with } \lambda \neq 0, 1 \end{aligned}$$

This is invariant under changing $\lambda \rightarrow \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}$. These six transformations form a group isomorphic to S_3 . So we have an affine variety given by

$$(\mathbb{A}^1 \setminus \{0, 1\})/S_3 \quad (\dagger)$$

Note $\mathbb{A}^1 \setminus \{0, 1\}$ is indeed an affine set since it is isomorphic to the curve $\lambda(\lambda - 1)\mu = 0$ in \mathbb{A}^2 where λ, μ are coordinates.

What is this space \dagger ? Well if we take the coordinate of this space here which is $k[\lambda, \frac{1}{\lambda}, \frac{1}{\lambda-1}]$ and take a subring that is invariant under the group S_3 of order six. In order to describe this we want to find some polynomial in these three coordinates that is invariant under S_3 this is the simplest one:

$$j = \frac{2^8(\lambda^2 - \lambda + 1)}{\lambda^2(\lambda - 1)^2} \quad (1)$$

And it turns out that $k[\lambda, \frac{1}{\lambda}, \frac{1}{\lambda-1}] \simeq k[j]$. This j is the so called j -invariant of an elliptic curve that we will study more later on.

11 Dimension

11.1 Defintions of Dimension

The concept of dimension is difficult to define precisely. Here are some definitions that were proposed

Definition 11.1. • **Dimension** is the number of parameters needed to define a point. This definition fails since \mathbb{R}^2 and \mathbb{R} have the same number of points and by Peano there are continuous maps from \mathbb{R} onto \mathbb{R}^2 . So in some sense points of \mathbb{R}^2 can be specified by only one parameter. This defintion works if we confine ourself to **smooth manifolds**.

- **Lebesgue covering dimension**, a set has dimension at most n if every open cover has a refinement so that each point is in at most $n + 1$ sets. So for example in \mathbb{R}^2 , if we cover the plane by open sets some points will be in three open sets but no points will be in four open sets. Lebesgue Convering dimension works fine in Euclidean space but not in algebraic geometry.
- **Brower, Menger, Urysohn's definition:** A topological space has dimension at most n where $n = -1, 0, 1, 2, \dots$ if all points have arbitrarily small nbhs whose boundary has dimension $< n$. For example if we take the plane we can take a small nbh around a point such that they have boundary of dimension 1. Traditionally this defintition is only used for seperable metric spaces, but spaces in alg geo are not seperable. But this definition works for algebraic sets!
- **Krull dimension:** Supremum of the numbers n for which there is a chain $Z_0 \subsetneq Z_1 \subsetneq \dots \subsetneq Z_n$ of *irreducible* subsets. For example if we look at a plane, Z_0 can be a point, Z_1 is a curve and Z_2 is the whole plane. This only works well for Noetherian spaces, since Haussdorff spaces all have Krull dimension 0 (since the only irreducible subsets are points). However for Noetherian spaces the Krull dimension is the same as the BMU dimension.
- **Various variations of the Haussdorff dimension:** The Haussdorff dimension is got by counting the number of balls used to cover a metric space and see what happens to the number of balls as the radius goes to zero, this dimension can take non-integer values. Though this does not seem useful in alg geo since we don't see many sets of non-integer dimensions here.
- **Transfinite dimensions:** Defintions such as the Krull and BMMU dimension can be extended so that they can be a countable or even uncountable ordinal. Again doesn't seem to be much of use in alg geo.
- **Deviation of poset** A poset has deviation at most α (an ordinal) if for all descending chains all the finite number of intervals of chain have deviation $< \alpha$. For Noetherian rings, we look at poset of ideals and deviation is equal to the Krull dimension. This definition works well for module, and non-commutative rings.

11.2 Algebraic defintion of dimension

The idea is that a set of high dimension has *many* functions on it. What do we mean by many? There are several ways of understanding what we mean by many:

Definition 11.2. • Suppose B variety over k Look at the quotient field of coordinate rings of B and we set $\dim(B) =$ transcendence dimensions of a quotient field. Where we recall a transcendence dimension is the largest amount of algebraically independant elements in the field. For example if $B = \mathbb{A}^2$, then the coordinate ring is $k[x, y]$, so the quotient field is $k(x, y)$ which has dimension 2. This definition works for algebraic varieties, but this doesn't work very well for other objects in alg geo like non-irreducible algebraic set or schemes.

- **Hilbert polynomial:** Recall a local ring is a ring with a unique maximal ideal \mathfrak{m} . For a local ring A , we look at the length of A/\mathfrak{m}^k which is a polynomial in k (for large k) of degree d . The dimesion of A is d . This defintion looks artificial but works well.
- **Gelfond-Kirillov dimension:** This applies to finietely generated algebras over a field, and is defined to be

$$\limsup_n \log(\dim R_n / \log(n))$$

Where R_n is generated by the monomials f length less than n . If R is commutative this is the same as the dimension from the Hilbert polynomial, if it is not a commutative it could be a real number ≤ 2 so again we can get a non-integral dimesion. Again this is not that useful in alg geo.

- **Dimesnsion of tangent space of a point:** This definition fails for varieties for singularites, but we can use this to define singular points. A space is non-singular at a point if the dimension of the tangent space is equal to it's dimension.
- **Minimal number of elements of system of parameters:** This defintion works but is not that intuitive.
- **Homological dimension:** We can define Homological dimension by asking when do various homology groups vanish.

To summarise for Noetherian topological spaces or Noetherian rings, there are several different ways of defining dimension, Krull dimension, Hilbert polynomial, BMU, system of parameters and for any reasonable object in algebraic geometry this will give us the same notion of dimension.

Lecture 3: Onwards, to Projective varieties!

12 Projective varieties

We will now move on from affine variety to projective varieties and start by defining projective space:

Definition 12.1. $\mathbb{P}^n(k) = \{1 \text{ dimensional subspaces of } k^{n+1}\}$, in other words each line in k^{n+1} corresponds to a point of \mathbb{P}^n as follows:

Coordinates of projective space are $(x_0 : x_1 : \dots : x_n) = (\lambda x_0 : \lambda x_1 : \dots : \lambda x_n)$ for not all $x_i = 0$ and $\lambda \in k \setminus \{0\}$

How does projective space looks like? If x_0 is non-zero:

$$(x_0 : \dots : x_n) = (1 : \underbrace{y_1 : \dots : y_n}_{\text{in } \mathbb{A}^n}) \text{ where } y_i = \frac{x_i}{x_0}$$

If $x_0 = 0$:

$$\underbrace{(0 : x_1 : \dots : x_n)}_{\text{in } \mathbb{P}^{n-1}}$$

So $\mathbb{P}^n = \text{disjoint union of } \mathbb{A}^n \text{ and } \underbrace{\mathbb{P}^{n-1}(k)}_{\text{"points at infinity"}}$

12.1 Projective space over the reals

Let $(x_0 : \dots : x_n) \in \mathbb{P}^n(\mathbb{R})$ we can rescale the points such that $x_0^2 + \dots + x_n^2 = 1$. So $(x_0 : \dots : x_n)$ correspond to points on a sphere but since $(x_0 : \dots : x_n) = (-x_0 : \dots : -x_n)$, opposite points are identified. So:

$$\mathbb{P}^n(\mathbb{R}) = S^n/\text{opposite points}$$

Example 12.1.1.

$$\mathbb{P}^0(\mathbb{R}) = \text{point}$$

$$\mathbb{P}^1(\mathbb{R}) = \text{circle}$$

$$\mathbb{P}^2(\mathbb{R}) = S^2/\text{opposite points} = \text{non-orientable surface}$$

12.2 Projective space over complex numbers

Let $(x_0 : \dots : x_n) \in \mathbb{P}^n(\mathbb{R})$ we can rescale the points such that $\underbrace{|x_0|^2 + \dots + |x_n|^2 = 1}_{\text{In } S^{2n+1}}$. But since this point is equal to $(\lambda x_0 : \dots : \lambda x_n)$ for $|\lambda| = 1$, from this we can make a map $S^{2n+1} \rightarrow \mathbb{P}^n(\mathbb{C})$, where the fibers are S^1 . We call this a fibration, in algebraic topology.

$$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} + \text{point} = \text{Riemann sphere} \simeq S^2 \text{ we are getting a fibration } \underbrace{S^1 \rightarrow S^3}_{\text{fibers}} \rightarrow S^2 \text{ this is the Hopf fibration}$$

Another example of a fibration would be:

$$S^1 \rightarrow S^1 \times S^2 \rightarrow S^2$$

We can also cover $\mathbb{P}^n(k)$ with copies of affine space \mathbb{A}^n , so $(x_0 : \dots : x_n)$ if we take $x_i \neq 0$ we get a copy of affine space. So all together we get $n+1$ copies of \mathbb{A}^n . So we shall think of projective space of glueing copies of affine space together.

12.3 Background of Projective geometry

What properties are preserved by projection? One property that isn't preserved is parallel lines (if we try to draw railway track, you will see the lines of the track meet at point at infinity).

There are two approaches to geometry:

Definition 12.2. 1. **Synthetic geometry** where we write out a set of axioms

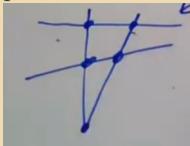
2. **Analytic geometry** where we use coordinates, and turn geometry into algebra

We have been discussing the analytic approach to projective geometry. But we can talk about synthetic geometry for projective geometry.

12.3.1 Synthetic approach to projective geometry

Axioms

1. Any two distinct points meet at unique line
2. Any two distinct lines in the “same plane” meet in one point. Two lines meet in a same plane if when we take four points on them and join them up like this:

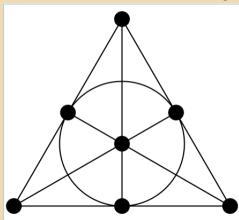


these two lines meet.

3. Any line meets at least 3 points. (this is a sort of non-degeneracy condition)

We can ask what object can we get satisfying these axioms.

- Dimension 0: point
- Dimension 1: Line + points
- Dimension 2: Projective plane, one example is the Fano plane, which has seven straight lines and seven points:



Notice one of the lines look like a circle.

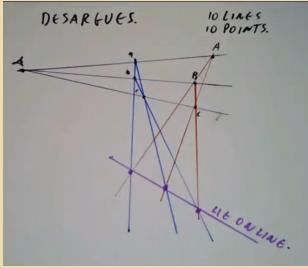
- Dimension ≥ 3 : $\mathbb{P}^n(k)$, over a field or division ring. (Note being a projective space over a field is equivalent to Pappus theorem).

So we don't get much by using axioms to describe projective space.

Remark. There are two sort of projective planes, Desargueian ones and non-Desargueian ones. These are planes relating to Desargues theorem.

12.3.2 Desargues' theorem

Theorem 15. Suppose we take a point (think of it as an observer), looking at a triangle ABC and drawing on some easel where they draw three points a, b, c which are the images of the points of the triangle they see. Join the lines ab and AB , bc and BC , ac and AC . So we have three points from these intersection, these points lie on a line.



Proof. Key point of the proof is to imagine abc and ABC in 3d space, with planes containing these triangles are different. Since the lines aA and bB meet then the lines ab and AB are on the same plane so meet at a point in space. Likewise the lines ac , AC and bc , BC meet in space.

So these three points are well defined in space, so these three points lie on the plane containing abc and the plane containing ABC , so these points meet in the intersection of these planes which is (usually) a line. (The intersection is not a line if the planes are equal but in that case we can take limits to still deduce the theorem) \square

If we got a projective space of dimension at least three, it automatically satisfies Desargues' theorem, but if we have a projective space of dimension two it may not satisfy Desargues' theorem.

Definition 12.3. Non-Desarguanian planes

These are projective planes that don't satisfy Desargues' theorem.

Desargues' theorem is in some sense equivalent to the associativity law for multiplication. We can set coordinates on a ring for a projective space and

$$\begin{aligned} \text{Desargues} &\iff \text{Associative} \\ \text{Pappus} &\iff \text{Commutative} \end{aligned}$$

So synthetic projective geometry is almost the same as analytic projective geometry, except for these non-desarguiian planes (one example is the projective plane is a plane over the ring of octonions).

12.4 Duality for projective space

Example 12.3.1. Let us look at a projective plane and the axioms:

- Any two distinct points meet in one line
- Any two distinct line meet in one point

So for any theorem we say about lines and points, we can find a dual theorem by replacing points with lines and vice-versa.

For example for Pascal's theorem:

- If we take three points given by intersecting pairs of lines they lie on a straight line.
- If we take three lines given by joining up pairs of points in three different ways then they meet at a point.

One way of thinking about duality is that it is just duality of vector spaces:

- points of \mathbb{P}^n correspond to lines of $\mathbb{A}^{n+1} = k^{n+1}$
- lines of \mathbb{P}^n correspond to planes of $\mathbb{A}^{n+1} = k^{n+1}$

For any vector space k^{n+1} we can take a dual space and if we have a line we can take a dual which will correspond to a hyperplane. So duality of projective space is closely related to taking the dual of the vector space.

13 Affine and projective varieties

Recall:

$$\begin{aligned} \text{Affine space} &\iff k[x_1, \dots, x_n] \\ \text{Affine alg subsets} &\iff \text{Radical ideal} \\ \text{Projective space} &\iff k[x_0, \dots, x_n] \text{ graded ring} \\ \text{Projective algebraic subsets} &\iff \text{Graded radical ideal} \end{aligned}$$

Where recall a graded ideal is one where every element is a sum of homogenous elements in the ideal; i.e. $p(x_0, \dots, x_n) = 0 \iff p(\lambda x_0, \dots, \lambda x_n) = 0$ (except (x_0, \dots, x_n)).

If we have a projective variety defined by various equations $p(x_0, \dots, x_n)$ we can look at the corresponding affine variety, invariant under scaling in \mathbb{A}^{n+1} define by the same equations.

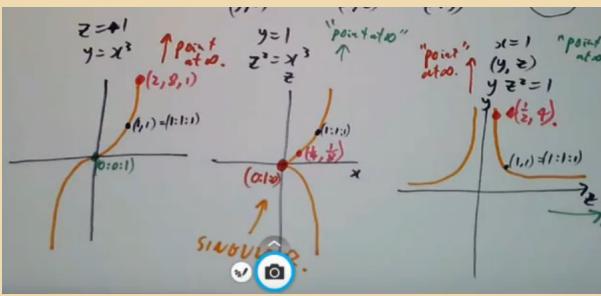
13.1 Examples

Example 13.0.1. Let us take the affine variety $y = x^3$ where $(x, y) \in \mathbb{A}^2$. To make it into a projective variety we look at points $(x : y : z) \in \mathbb{P}^2$, where $(x, y) \leftrightarrow (x : y : 1)$. In order to define a closed subset of projective space we need to make our polynomial homogenous, so we add in powers of z :

$$yz^2 = x^3$$

Recall that: \mathbb{P}^2 is covered by three copies of affine space: $x = 1$ (yz -plane) or $y = 1$ (xz -plane) or $z = 1$ (xy -plane), here we have a curve living in projective space we will look at the restriction of this curve in each copy of affine space:

- $z = 1, y = x^3$
- $y = 1, z^2 = x^3$
- $x = 1, yz^2 = 1$



The point $(0: 0: 1)$ in the graph $z = 1$, becomes the point at infinity in $y = 1$ and a point at infinity for $x = 1$. Likewise for the point $(0: 1: 0)$ in the graph $y = 1$.

All other points appear on all three diagrams. Note the second diagram has a wonky point at a cusp, that is a singular point.

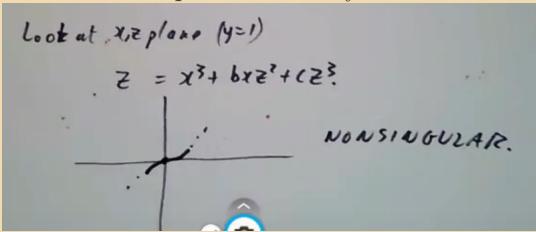
Example 13.0.2. Let us look at the elliptic curve:

- Affine: $y^2 = x^3 + bx + c$, (x, y)
- Projective: $y^2z = x^3 + bxz^2 + cz^3$, $(x: y: z)$

If we take

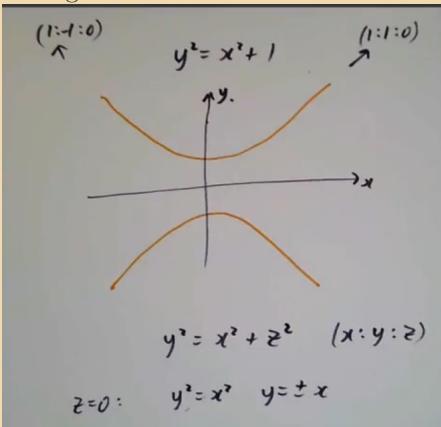
- $z = 1$, then we get $y^2 = x^3 + bx + c$
- $z = 0$: then $x^2 = 0 \Rightarrow x = 0$, so the only point at infinity is the point $(0: 1: 0)$.

How does this point at infinity look like?



Example 13.0.3. Example with more than one point at infinity:

Look at the curve $y^2 = x^2 + 1$, we can guess infinite points $(1: 1: 0)$ and $(1: -1: 0)$. If we want to be rigorous it is easy, we homogenize it.



13.1.1 Twisted Cubic

In affine space this is the set of points of the form $(t, t^2, t^3) = (x, y, z)$. We want to look at the ideal that defines this curve, which we can see by inspection is: $(y - x^2, z - x^3)$. What is the closure of this in \mathbb{P}^3 ?

The WRONG answer Let's homogenize the generators!

$$(wy - x^3, w^2z - x^3) \in k[w, x, y, z]$$

This defines something in \mathbb{P}^3 . Notice there is something fishy going on, the original ideal contains $y^2 - zx$ and $z - xy$ but our ideal doesn't contain $y^2 - zx$ or $wz - xy$.

We can't just homogenize an ideal by homogenizing a set of generators! We need to homogenize all elements of the ideal.

The CORRECT answer In projective space the twisted cubic's closure is given by $(s^3 : s^2t : st^2 : t^3)$ (so it is the curve $s = 1$ plus an extra point $s = 0$). We can check that the ideal of polynomials that vanish on this is the ideal:

$$(wy - x^2, y^2 - zx, wz - xy)$$

What algebraic set in projective space does $(wy - x^2, y^2 - zx, wz - xy) \in k[w, x, y, z]$ represent? Well \mathbb{P}^3 is covered by four copies of \mathbb{A}^3 with $w = 1, x = 1, y = 1$ or $z = 1$.

- $w = 1$: $y - x^2 = 0, z - x^3 = 0$, the twisted cubic
- $x = 1$: $wy = 1, w^2z = 1$, affine z -line minus a point
- $y = 1$: $w = x^2, w^2z = x^3$; substituting w in the second equation we get:

$$x^4z - x^3 = 0 \Rightarrow x^3(zx - 1) = 0$$

So we get a “triple” line at $x = 0 = w$.

- $z = 1$, similar to above we pick up the curve with a strange triple line.

So if we take our cubic in affine space, and try to make it a part of projective space in this careless way we pick up a triple line at infinity, which is not what we wanted! The fact that this contains two components corresponds to the Lasker-Noether style decomp of this ideal:

$$(wy - x^2, y^2 - zx, wz - xy) = \underbrace{(wy - x^2, y^2 - zx, wz - xy)}_{\text{the line we want}} \cap \underbrace{(wy - x^2, w^2, wx)}_{\text{corresponds to triple line at infinity}}$$

14 Product of varieties

First of all:

$$\begin{aligned} \mathbb{A}^m \times \mathbb{A}^n &= \mathbb{A}^{n+m} \\ (x_1, \dots, x_m) (y_1, \dots, y_n) &\rightarrow (x_1, \dots, x_m, y_1, \dots, y_n) \\ k[x_1, \dots, x_m] k[y_1, \dots, y_n] &\rightarrow k[x_1, \dots, x_m] \otimes k[y_1, \dots, y_n] = k[x_1, \dots, x_m, y_1, \dots, y_n] \end{aligned}$$

For algebraic sets, suppose X is defined by the ideal I and Y by J then $X \times Y$ is defined by the ideal (I, J) .

14.1 Product of projective space

Is $\mathbb{P}^m \times \mathbb{P}^n$ equal to \mathbb{P}^{n+m} ? NO! Since $S^1 \times S^1 = \mathbb{P}^1(\mathbb{R}) \times \mathbb{P}^1(\mathbb{R})$, but this is not equal to $\mathbb{P}^2(\mathbb{R})$, since the first set is orientable but the second one isn't.

What if we use maps? If we try to make a map $(x_0 : \dots : x_m) (y_0, \dots, y_n) \rightarrow (x_0 : x_1 : \dots : x_m : y_1 : \dots)$. This does not make sense since it is not well defined! We can scale $(x_0 : \dots)$ by λ and $(y_0 : \dots)$ by μ , and the result makes no sense.

But note we can create a map:

$$\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\text{not onto}} \mathbb{P}^{mn+m+n}$$

$$(x_0 : \dots : x_m) \cdot (y_0, \dots, y_n) \rightarrow (x_0 y_0 : x_1 y_0 : \dots : x_m y_0 : x_0 y_1 : \dots : x_m y_n : y_1 : \dots) = (w_{00} : w_{10} : \dots : w_{m0} : \dots : w_{mn})$$

Where we have the relations $w_{ij} = x_i y_j$ and $w_{ij} w_{kl} = w_{il} w_{kj}$

Remark. More abstract way of defining this map is by

$$\begin{aligned} k^{m+1} \times k^{n+1} &\rightarrow k^{m+1} \otimes k^{n+1} \\ (v, w) &\rightarrow v \otimes w \end{aligned}$$

We want to show the map:

$$\mathbb{P}^m \times \mathbb{P}^n \rightarrow \{(w_{00} : w_{10} : \dots : w_{m0} : \dots : w_{mn}) \mid w_{ij} w_{kl} = w_{il} w_{kj}\}$$

this map is the Segre embedding

Is onto.

We can assume (by rearranging terms if need be) that $w_{00} = 1$. So we have $w_{kl} = w_{0l} w_{k0} = y_l x_k$ since $x_0 = y_0 = 1$

So the product of two projective spaces is a projective variety! By more or less comparing the argument for affine spaces we can see that the product of any projective variety is a projective variety.

14.2 Example of the Segre map

$$\begin{aligned} \mathbb{P}^1 \times \mathbb{P}^1 &\rightarrow \mathbb{P}^3 \\ (x_0: x_1), (y_0: y_1) &\rightarrow (x_0y_0: x_0y_1: x_1y_0: x_1y_1) = (w_0: w_1: w_2: w_3) \end{aligned}$$

With $w_0w_3 = w_1w_2$, which is a quadric in \mathbb{P}^2 . Over any algebraically closed field with characteristic not equal to 2, any two nonsingular quadrics are isomorphic, and they must be of the form $x_0^2 + x_1^2 + \dots + x_n^2 = 0$.

So any quadric in \mathbb{P}^3 is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, so it got two lines on it. For example if we take the sphere $x^2 + y^2 + z^2 = 1$, we claim it has straight lines over \mathbb{C} ! For example $x = 1, y = iz$

Exercise 1

Find all straight lines on $x^2 + y^2 + z^2 = 1$ over \mathbb{C} , (note $(x+iy)(x-iy) = (1-z)(1+z)$)

15 Two examples of Projective Varieties

15.1 Veronese surface

This contains of all points of the form

$$(x^2: xy: xz: y^2: yz: z^2) \in \mathbb{P}^5$$

We can look at this as a map from $\mathbb{P}^2 \rightarrow \mathbb{P}^5$, obviously this map is not onto. We would like to describe the subset of \mathbb{P}^5 by finding explicit formula for it.

So we take $(w_{00}: w_{01}: w_{02}: w_{11}: w_{12}: w_{22}) \in \mathbb{P}^5$. Note that the map satisfies $w_{ij}w_{kl} = w_{ik}w_{jl}$, and $w_{ij} = w_{ji}$.

We can check that the map is onto.

We can also take of this map as from $\mathbb{A}^3 \rightarrow \mathbb{A}^6$, where we can think of \mathbb{A}^6 as $S^2(\mathbb{A}^3)$, where $S^2(\mathbb{A}^3)$ is the set of all degree two monomials in $\{x, y, z\}$ where this is the basis of \mathbb{A}^3 .

15.2 Variety of all lines in \mathbb{P}^3

What does the dimension of this variety be? If we take a line in \mathbb{P}^3 and a random plane, then the line will pass through some point in the plane (2 degrees of freedom) and then it can point in a direction in ordinary Euclidean space, this direction is given by a point on the sphere S^2 , which gives us 2 more degrees of freedom.

So we expect the dimension of this variety to be of dimension 4. A line in $\mathbb{P}^3 \iff 2 - \dim$ subspace of k^4 . This is a special case of what is called a Grassmannian.

Definition 15.1. The **Grassmannian** $G(m, n)$ is the set of all m dimensional subspaces of k^{m+n} .

For example:

- $G(0, m) = G(m, 0) = \text{point}$
- $G(1, m) = \mathbb{P}^m$
- $G(m, n) \simeq G(n, m)$. Indeed since we have m dimensional subspace $k^{m+n} \xrightarrow{\text{dual}} (k^{m+n})^* \simeq k^{m+n}$ n dimensional subspace
- So $G(m, 1) = \mathbb{P}^m$
- The first non-trivial case that isn't a point or projective space is

$$G(2, 2) = 2 - \dim \text{subspaces of } k^4$$

In general, grassmannians are special cases of Hilbert schemes, these are schemes (we will discuss this later) whose points correspond to certain configurations of projective space satisfying certain conditions. The simplest condition is that it must be a linear subspace of projective space. So grassmannians are the simplest examples of Hilbert schemes.

We will embed $G(2, 2)$ into \mathbb{P}^5 .

Pick a line in \mathbb{P}^3 corresponding to a point of $G(2, 2)$. Pick two distinct points on the line, $(a_0: a_1: a_2: a_3) \neq (b_0: b_1: b_2: b_3)$, now we create a two by four matrix from these two points:

$$\begin{pmatrix} a_0: a_1: a_2: a_3 \\ b_0: b_1: b_2: b_3 \end{pmatrix}$$

Let $s_{ij} = \det$ of columns i, j ; for example $s_{01} = \det \begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix} = a_0b_1 - a_1b_0$

So we get six coordinates: $(s_{01}: s_{02}: s_{03}: s_{12}: s_{13}: s_{23})$, note that $s_{30} = \lambda s_{03}$ for some λ , we also see $s_{ii} = 0$ so we can ignore these.

Notice that this point \mathbb{P}^5 only depends on the line we have chosen. If we multiply all the a's or b's by a constant all these determinants are multiplied by a square of that constant so the point is the same. Secondly we had a lot of choice of which two points we placed on the line, we can pick other points by replacing b by a multiple of a, which is equivalent to adding a multiple of the first row to the second row which won't change the determinant, so it won't change the point in \mathbb{P}^5 .

So we have a well defined map from lines in P^3 to points in \mathbb{P}^5 . Note that by checking dimensions we can clearly see that this map is not onto. So what is the relation between these s_{ij} ? It's the Plucker Relation.

Plucker Relation

$$s_{01}s_{23} - s_{02}s_{13} + s_{03}s_{12} = 0$$

(Proof that this relation holds, is that each term of the form $a_i b_j - a_j b_i$ occurs twice with opposite signs).

Are there any other relation satisfying these points? No! If we got a set of numbers satisfying the plucker relation there is a line in $G(2, 2)$ corresponding to that point.

Showing the map $G(2, 2) \rightarrow$ solutions of the plucker relation is onto Some s_{ij} must be non-zero, so we can assume it is 1. So we may assume that $s_{01} = 1$. But notice that:

$$s_{01}s_{23} = s_{02}s_{13} - s_{03}s_{12}$$

So s_{23} is determined by $s_{02}, s_{13}, s_{03}, s_{12}$. So pick the two points:

$$\begin{aligned} & (1: 0: s_{12}: s_{13}) \\ & (0: 1: s_{02}: s_{03}) \end{aligned}$$

These two points determine a line in $G(2, 2)$ which maps to the given point in \mathbb{P}^5 .

15.2.1 Find cohomology of quadric in \mathbb{P}^5

Notice that the Grassmannian is the union of the following subsets:

$$\left(\begin{matrix} 1: 0: *: * \\ 0: 1: *: * \end{matrix} \right), \left(\begin{matrix} 1: *: 0: * \\ 0: 0: 1: * \end{matrix} \right), \left(\begin{matrix} 1: *: *: 0 \\ 0: 0: 0: 1 \end{matrix} \right), \left(\begin{matrix} 0: 1: 0: * \\ 0: 0: 1: * \end{matrix} \right), \left(\begin{matrix} 0: 1: *: 0 \\ 0: 0: 1: * \end{matrix} \right), \left(\begin{matrix} 0: 0: 1: 0 \\ 0: 0: 0: 1 \end{matrix} \right)$$

These form six copies of various affine space, $A^4, A^3, A^2, A^2, A^1, A^0$ respectively. The dimension of the cohomology groups can be read out from these.

We can also use this answer an alternative question:

How many points does $G(2, 2)$ have over a FINITE field k Note that A^n has q^n points, ($q = |K|$).

So $G(2, 2)$ has

$$q^0 + q^1 + 2q^2 + q^3 + q^4 \text{ points}$$

While

$$\mathbb{P}^4 = q^0 + q^1 + 2q^2 + q^3 + q^4 \text{ points}$$

So there is some relation between cohomology group of a variety over complex numbers and the number of points of the variety over a finite field. This is the theme of the **Weil conjectures** of a variety over a finite field.

16 Grassmannians

Let's now look at more general grassmannians $G(m, n)$.

Theorem 16. $G(m, n) \subseteq \mathbb{P}^{\binom{m+n}{n}-1}$

Proof. Suppose given some m -dimensional subspace of k^{m+n} , pick m vectors spanning it and create a matrix of size $m(m+n)$.

$$\begin{pmatrix} a_1 & \dots & a_{m+n} \\ b_1 & \dots & b_{m+n} \\ b_1 & \dots & b_{m+n} \\ \vdots & & \end{pmatrix}$$

Where each row form the coordinates of one these points. Now pick any m columns and look at the determinant of these columns (so the determinant of an $m \times m$ minor of this matrix). So this gives us $\binom{m+n}{m}$ numbers, let's call these numbers $p_{i_1 \dots i_m}$ if we picked columns i_1, \dots, i_m , So these give points in $\mathbb{P}^{\binom{m+n}{n}-1}$. \square

Remark. More abstract way of showing this:

Suppose we have a vector space V of dimension m which is a subspace of W of dimension m, n .

Taking the m^{th} exterior power of V we can find a map:

$$\underbrace{\Lambda^m V}_{\dim=1} \rightarrow \underbrace{\Lambda^m W}_{\dim=\binom{m+n}{n}}$$

So whenever we have an m dimensional of a $m + n$ dim space, we have a corresponding 1 dimensional space of a $\binom{m+n}{n}$ dimensional space. This corresponds to a point of the projective space $\mathbb{P}(\Lambda^m W)$.

Of course this is map is not onto, we have some plucker relations.

16.1 Plucker relations:

$$\sum_{\lambda} (-1)^{\lambda} p_{i_1 \dots i_{m-1}, j_{\lambda}} p_{j_1 \dots j_{\lambda-1}, j_{\lambda+1} \dots j_{m+n}} = 0$$

This equality is true since every monomial occurs twice with opposite signs. So notice the Plucker relations f a lot of quadric relations.

Theorem 17. *The map $G(m, n) \rightarrow$ space of zeroes of plucker relations is onto.*

Proof. We can assume that $p_{1 \dots m} = 1$ by changing coordinates if necessary. Then we can find a point in the grassmannian with given values of:

$p_{1 \dots r-1, r+1 \dots m, s}$ by choosing a matrix whose left comes from the identity

But then plucker relations determine all the other p 's. \square

16.2 Applications

There are several applications of grassmannians.

- Grassmannians are covered by affine spaces.
- Product of Grassmannians are given by the Littlewood-Richardson rule.
- “Line complexes”, these are certain varieties with a rich structure. The quadric line complex is given by $G(2, 2) \subseteq \mathbb{P}^5$ and we intersect it with a quadric in \mathbb{P}^5 . (cf. last chapter Griffiths & Harris Algebraic Geometry)
- $G(m, n) = GL_{m+n}(k) / \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

Note that $GL_{m+n}(k)$ and $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ are affine, but their quotient $G(m, n)$ may not be affine since it is a projective variety.

In fact the quotient of two affine varieties doesn't always have to be affine or projective for example, suppose we take: $k^2 \setminus (0, 0)$, this variety is neither affine, nor projective. But $GL_2(k)$ acts transitively on it and the subgroup fixing a point is $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, which is an affine line.

So $k^2 \setminus (0, 0) = GL_2(k) / \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, is a quotient of affine group by affine group but is neither affine nor projective.

- Construction of Hilbert Scheme by Grothendieck, the idea of the Hilbert scheme is that it parameterizes subschemes of projective space. What does this mean? We take coordinate ring of projective space $k[x_0, \dots, x_n]$ and we take graded ideals $I = 0 \oplus I_1 \oplus I_2$. So we want to classify graded ideals of this ring and in particular we want to show that graded ideals correspond to points of some projective space. We will see later that $\dim(I_j)$ is a polynomial in j , for j large (It's more or less the Hilbert polynomial). Suppose that I_d generates I_{d+1}, I_{d+2}, \dots , so $I_d \subseteq S_d$ (degree d monomials), which is a point of a grassmannian which is itself contained in some large projective space.

16.3 Why is the mapping natural?

Now what do we mean by there is a **natural** mapping between the lines in \mathbb{P}^3 and the points of $G(2, 2) \subseteq \mathbb{P}^5$. Notice in some sense it is trivial to find a variety whose points correspond to lines in \mathbb{P}^3 , all we need to do is to find a variety of the same cardinality and take a bijective map. But this is a useless correspondence, we want that makes sense.

How do we define a natural correspondence? This was defined by Grothendieck, look at **functors** from commutative rings R .

- $F: R \rightarrow \text{Lines in } \mathbb{P}^3(R)$
- $R \rightarrow G(2, 2)$ over R
- $G: R \rightarrow R\text{-valued points of a quadric given by the plucker relation } p_{01}p_{12} + \dots + \dots = 0 \text{ in } \mathbb{P}^5$

Grothendieck's way of saying that the lines in \mathbb{P}^3 correspond naturally to the points of the above quadric, says that these three are **ISOMORPHIC AS FUNCTORS**

So not only $F(R), G(R)$ are isomorphic as sets, but if we have a morphism $R \rightarrow S$ we can create this commuting diagram

$$\begin{array}{ccc} F(R) & \longrightarrow & F(S) \\ \text{iso} \downarrow & & \downarrow \text{iso} \\ G(R) & \longrightarrow & G(S) \end{array}$$

In order for all of this to make sense we need to work over general commutative ring R , it is not enough to work over fields.

More generally Grothendieck showed that any scheme is defined by its functor of points.

17 More examples of projective varieties: Projective space bundles

Definition 17.1. Recall a **fibre bundle** is a space that looks locally like a product space. So assume we have a space E (total space), F (the fibre), B (the base space of the bundle). Such that there is a surjective map $E \rightarrow B$.

Then for small open sets $U \subseteq B$, we have U looks locally like the projection $F \times U \rightarrow U$

Example 17.1.1. Let $B = S^1$, and $F = \mathbb{R}^1$, then we can map $S^1 \times \mathbb{R} \rightarrow S^1$. This will be a special case of a fibre bundle (it will look like a cylinder mapping to a circle).

On the other hand we can map a Moebius Band $\rightarrow S^1$, where we can think of the Moebius bands projected on a circle where the fibres are copies of \mathbb{R} . Locally this map looks like a product, if we take a small piece of a circle its pre-image looks like the product of \mathbb{R} and this little piece. But notice that while locally the Moebius band looks like a product, globally it doesn't.

Fibre bundles are sort of twisted products. Quite often the Fibre is a vector space in this case we talk about **vector bundle**. If the Fibre is a copy of projective space we talk about a **projective space bundle**.

17.1 Hirzebruch surfaces

Let us look at the space:

$$(\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^2 \setminus 0) \text{ acted on by } G_m \times G_m$$

Where $G_m = \mathbb{C}^*$. So if we let G_m take $(x, y) \rightarrow (\lambda x, \lambda y)$ \mathbb{A}^2/G_m , then $(\mathbb{A}^2 \setminus 0)/G_m = \mathbb{P}^1$. So if we take the obvious action we see that $(\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^2 \setminus 0)/G_m \times G_m = \mathbb{P}^1 \times \mathbb{P}^1$.

But we can let G_m act in another way:

$$\underbrace{(\lambda, \mu)}_{G_m \times G_m} \underbrace{((s, t), (x, y))}_{(\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^2 \setminus 0)} = (\lambda s, \lambda t, \mu x, \lambda^{-a} \mu y), \text{ where } a \in \mathbb{Z}$$

Now under this action $F = (\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^2 \setminus 0)/G_m \times G_m$, is called the Hirzebruch surface.

There is a map $F \rightarrow \mathbb{P}^1$ given by $(s, t, x, y) \rightarrow (s : t)$. Similarly the fibre at any point is also isomorphic to \mathbb{P}^1 . We can check that locally this is a product but globally it is not a product. We have a surface that is a fibre bundle of \mathbb{P}^1 , whose fibres are also copies of \mathbb{P}^1 . It is a kind of “twisted” copy of $\mathbb{P}^1 \times \mathbb{P}^1$.

17.2 Scrolls

We act on $(\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^n \setminus 0)$ by $G_m \times G_m$ where:

$$(\lambda, \mu)(s, t, x_1, \dots, x_n) = (\lambda s, \lambda t, \lambda^{-a_1} \mu x_1, \lambda^{-a_2} \mu x_2 \dots), \text{ where } a_i \in \mathbb{Z}$$

The **Scroll** is given by the quotient $(\mathbb{A}^2 \setminus 0) \times (\mathbb{A}^n \setminus 0)/G_m \times G_m$.

Note just as before we get a map from the scroll to \mathbb{P}^1 by taking $(s, t, x_1, \dots, x_n) \rightarrow (s: t)$ and the fibres are copies of \mathbb{P}^{n-1} .

Let's map this to projective space: Assume that all the $a_i > 0$, then we can consider the monomials:

$$s^i t^{a_j 0 - i} x_j \text{ for } j = 1, 2, \dots, n \text{ and } 0 \leq i \leq a_j$$

We can consider these as points in $\mathbb{P}^{(\sum a_j + 1) - 1}$, we can see that each of these fibres are mapped to a linear subspace of this projective space.

It's a bit clumsy to have to map everything into projective space, it is sometimes useful to use "abstract algebraic varieties".

17.2.1 Abstract varieties (Weil)

Weil defined them in order to do a construction called doing the "Jacobian of a curve", it wasn't obvious at the time that these objects were embeddable in projective space. So he came up with this concept which let him construct varieties without having to embed them into projective space.

Differentiable manifolds

- **The old view:** Subset of \mathbb{R}^n defined by some equations. For example $S^2 =$ points such that $x^2 + y^2 + z^2 = 1$ in \mathbb{R}^3 . But this is not really a differentiable manifold, it is a differentiable manifold with an embedding into Euclidean space. We don't think of differentiable manifolds as coming with embeddings of Euclidean space anymore.
- **The new view:** We think of covering our manifold by charts. For example we might cover S^2 with two pieces, each of these pieces which look like an open disk in Euclidean space. So we might think of S^2 as two open disks which are glued together.
-

Bringing this into algebraic geometry

- **The old view:** Variety is a subset of \mathbb{P}^n defined by equations.
- **The new view:** Take some AFFINE varieties and glue them together.

For example \mathbb{P}^1 can be thought as two copies of the affine line \mathbb{A}^1 glued together. (We can find copies $\mathbb{A}^1 = (1: y)$ and $\mathbb{A}^1 = (x: 1)$) How do we glue them together? we take the subsets $\mathbb{A}^1 \setminus 0$ from each copy and glue them by mapping $x \rightarrow \frac{1}{y}$, where $x \in \mathbb{A} \setminus 0$ and y is in the other copy.

What happens when you glue them by the map $x \rightarrow y$, then we are identifying all the non-zero points together so we get something that looks like the line with two origins (non-Hausdorff space).

This gives an example of an abstract variety that isn't a projective variety, abstract varieties are more general than projective varieties. It turns out all "reasonable" abstract varieties (i.e. that ignoring these kind of varieties) in dimension 1 are projective varieties, in 2 dimensions if they don't have singularities are projective. But there are some 3 dimensional examples of non-singular, non-projective abstract varieties.

17.3 Toric varieties

We will start with an example of how to construct affine varieties from cones.

17.3.1 2 dimensional example

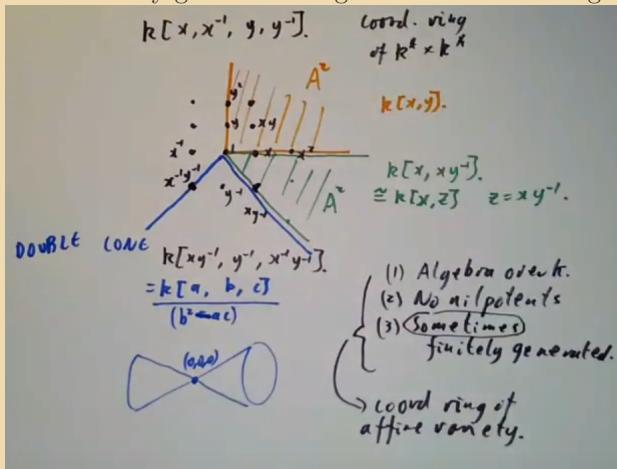
We start with $k[x, x^{-1}, y, y^{-1}]$ which is the coordinate ring of $k^* \times k^*$ (note even though the non-zero points in k don't form an algebraic set, we can think of them as points on a hyperbola). If we draw a picture of this ring we get a sort of lattice. By defining cones we can take the subring generated by monomials on that cone.

Whenever we take a subring generated by a cone it has the following properties:

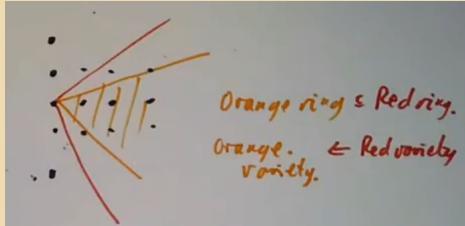
1. Algebraic over k

2. No nilpotent
3. It is sometimes finitely generated. It is fin gen if it “rational”, if its edges passes through a rational point in the two dimensional case.

If it is finitely generated we get the coordinate ring of an affine variety.

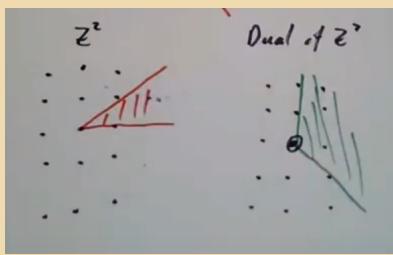


What happens to varieties associated to certain cones? Suppose we take two cones as in the picture. What is the relation between the corresponding varieties. We get a map from the orange ring to the red ring; so the maps from the varieties go in the opposite directions. This is a bit annoying since we would prefer a map from the orange variety to the red one.



We can get around this by using duality:

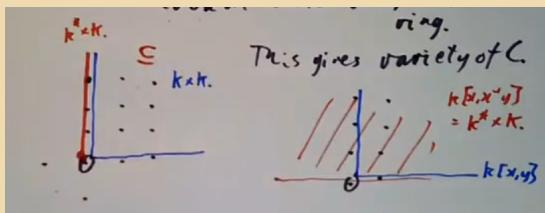
Definition 17.2. If we have a lattice \mathbb{Z}^2 we can look at the dual lattice, where every cone in \mathbb{Z}^2 we can look at the **dual cone**; which are the points on the dual of \mathbb{Z}^2 which are positive on the cone. If a cone is contained in another cone their dual cones will have the containment reversed.



Instead of associating a variety to a cone we associate a variety by taking the ring associated to its dual cone. For each cone C in \mathbb{Z}^2 look at the dual cone and take the corresponding ring. This gives the variety of C .

Example 17.2.1. The cone that is the line like in the picture has dual cone the half-plane. The coordinate ring of the half-plane is $k[x, x^{-1}, y]$ which corresponds to the variety $k^* \times k$:

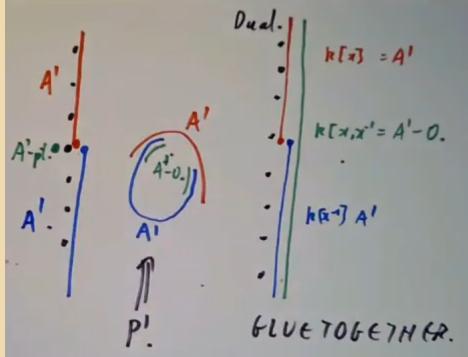
On the other hand if we take a quadrant, its dual will be the same quadrant which corresponds to $k[x, y]$ which is $k \times k$, So the inclusion order for varieties and cones are the same!



Another example with an interesting conclusion Now we can look at several cones in 1 dimension:

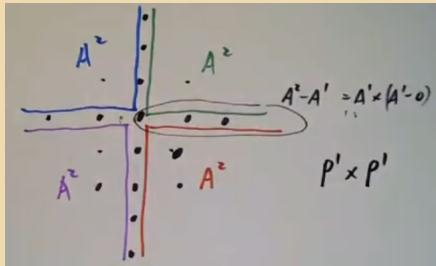
Example 17.2.2. The red cone which is a line, the blue cone which is the opposite line and the green cone, their intersection which is their intersection a point. The dual of the red and blue cones are the same but the dual of the green cone is the whole line.

These give us three varieties, two copies of \mathbb{A}^1 and a copy of $\mathbb{A} \setminus 0$, we can glue them together to get \mathbb{P}^1 .

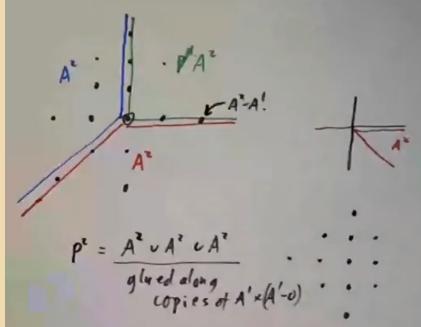


Now let us look in two dimensions:

Example 17.2.3. If we split the lattice into four quadrants we see that our image is the product if two copies of the figure we had in the last example, so we get not \mathbb{P}^2 but $\mathbb{P}^1 \times \mathbb{P}^1$. The varieties we get like this are sometimes called **Toric varieties**

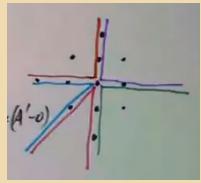


Getting \mathbb{P}^2 with cones

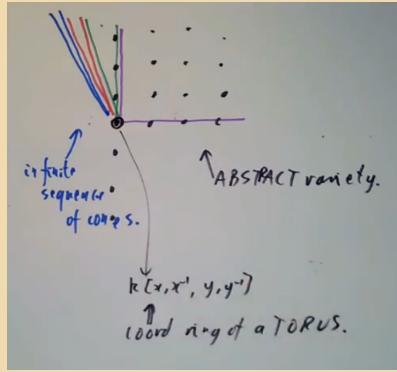


We are gluing together three copies of \mathbb{A}^2 along the intersections $\mathbb{A}^1 \times \mathbb{A}^1 \setminus 0$

Exercise 1 What is this?



Abstract Varieties We can also find some more exotic examples, for example in the image here, we are glueing an infinite sequence of cones. What project variety do we get? We don't get one! It is too big to be a projective variety, in fact it is not quasi-compact. It is an abstract variety.



Toric varieties The sort of varieties we get like this are called **Toric varieties**, since they all contain a torus as a dense subvariety.

If we take any collection of cones we can look at a single point, the variety of this point will map to the abstract variety we have since it is contained in all cones.

In two-dimension the point maps to $k[x, x^{-1}, y, y^{-1}]$ which is the **coordinate ring of a torus**.

Why is this called a torus? Recall from algebraic topology a torus is the product of any number of copies of S^1 . I.e. $(S^1)^n$

We can form S^1 over the reals, it will be the set $x^2 + y^2 = 1$, over the complex numbers this gives us $(x + iy)(x - iy) = 1 = z_1 z_2$ is a hyperbola isomorphic to $\mathbb{C} \setminus 0$

So \mathbb{C}^* is an analogue of S^1 . More generally over the complex numbers we can call $(\mathbb{C}^*)^n$ a **torus**. A torus of this form plays the same role as the ordinary torus plays in the theory of compact Lie Groups.

So toric varieties all have a torus like this as a dense subset.

Lecture 4: Morphisms

18 Category Theory

Definition 18.1. A **category**, Is a collection of *objects* and *morphisms*, such that for any two objects there is a set of morphisms between them, And such that the following conditions hold:

1. Given objects A, B, C ; $f: A \rightarrow B$, $g: B \rightarrow C$, are morphisms then there is a morphism $g \circ f: A \rightarrow C$ (**composition of morphisms**),
2. For each object A , there is an identity morphism, such that the composition of a morphism f and the identity gives f .
3. When defined composition is associative

A category is usually named after it's objects,

Definition 18.2. An **isomorphism** is a morphism that has two sided inverse, under composition.

18.1 Examples

For example we have:

- *Category of sets*, with morphisms the set of *functions* from A to B ; for sets A and B
- *Category of groups* with morphisms the *homomorphisms*.
- *Category of topological spaces* with morphisms the *continuous functions*.
- *Category of Commutative ring* with morphisms the *homomorphisms of rings*.

How do we define a product of two objects?

Definition 18.3. Suppose we have two objects A, B . Then we define the **product**, $A \times B$, to be an object with maps $A \times B \rightarrow B$ and $A \times B \rightarrow A$, which is *universal* with this property. I.e. for any object C with given morphisms $C \rightarrow B$, $C \rightarrow A$. Then there is a unique morphisms $C \rightarrow A \times B$ such that this diagram commutes:

$$\begin{array}{ccc} C & \xrightarrow{\quad} & A \times B & \xrightarrow{\quad} & B \\ & \searrow & \downarrow & \nearrow & \\ & & A & & \end{array}$$

Note the product is NOT unique, but is unique upto **unique isomorphism**. Indeed if we have A, B and X, Y were two objects with this universal property then:

$$\begin{array}{ccccc} X & \xleftarrow{\quad} & A \times B & \xrightarrow{\quad} & B \\ \psi \swarrow & \nearrow \phi & \downarrow & \searrow & \\ Y & \xrightarrow{\quad} & A & & \end{array}$$

Where ϕ is unique that making all the diagrams commute, and ψ is a unique map making all the diagrams commute. So the composition of these two maps is a map from Y to itself making these diagram commute so it must be the identity.

Exercise 1 The product of sets, topological spaces, and of rings. All have this universal property.

18.2 Varieties and Categories

We want to turn varieties and algebraic sets into categories. There are two ways of doing this:

- Using regular maps (analogue of smooth maps)
- Using rational maps

Definition 18.4. The **opposite** category is given by reversing all arrows in the morphisms. So for a category C the opposite category C^0 is such that the morphisms from A to B are the same morphisms of C from B to A .

This is a sort of generalization of the dual of a vector space.

Proposition 1. We will see that Affine varieties and regular maps are **dual** to the category of finite algebras over k with no nilpotents.

If we have a map $V \rightarrow W$, we get a map functions on $V \leftarrow$ functions on W .

18.2.1 Regular functions

Definition 18.5. For an affine variety $Y \subseteq \mathbb{A}^n$ is defined by some ideal I and the coordinate ring of Y is $k[x_1, \dots, x_n]/I$, this coordinate ring is the ring of **regular functions** on Y . We can think of this as the restriction of polynomials to Y .

More generally we want to define a regular function for U open in Y , we call U quasi-affine.

Example 18.5.1. • $U = \mathbb{A}^1 \setminus 0$, so $U \simeq \{xy = 1 \text{ in } \mathbb{A}^2\}$. In this case we want x^{-1} to be regular on U , so we want the ring of regular function to be $k[x, x^{-1}]$.

- $U = \mathbb{A}^2 \setminus (0, 0)$, which is not any affine variety.

Definition 18.6. A function $f: U \rightarrow k$, where U is quasi-affine, is *locally regular* at $o \in U$, if $f = \frac{g}{h}$ in some nbh of p where g, h are polynomials and $h \neq 0$ at p .

Note that g, h may depend on p .

Definition 18.7. A **regular function** on a quasi-affine variety U , is a function (to k) that is *locally regular* at all points $p \in U$.

Problem: Suppose Y is affine, are locally regular functions (regular at each point), globally regular (polynomials in \mathbb{A}^n)?

Since Y is affine it is compact, assume that $Y = U_1 \cup U_2 \cup \dots \cup U_n$, where U_i are open. Furthermore, since the sets of the form $Y \setminus V(F)$ form a basis for the Zariski topology of Y , we can assume that each of the open sets $U_i = Y \setminus V(f_i)$ for some polynomial f_i .

Let f be a function on Y , such that f is regular on all U_i .

$$f = \frac{g_i}{h_i}, \text{ on } U_i, \text{ with } g_i, h_i \text{ polynomials and } h_i \neq 0 \text{ on } U_i$$

Proposition 2. f is a polynomial

Proof. Note that since Y is covered by U_i , no point of Y is outside all the U_i so no maximal ideal of $k[x_1, \dots, x_n]$ containing I contains all the h_i (since if so we would have a point of Y that is zero on all the h_i , so it would not be in any of the U_i by definition of h_i .)

Therefore, the ideal generated by h_1, h_2, \dots and I is the unit ideal. Therefore:

$$1 = a_1h_2 + a_2h_2 + \dots + a_nh_n \pmod{I}, \text{ for some polynomials } a_i$$

By multiplying both sides by f we get:

$$\begin{aligned} f &= a_1h_1f + a_2h_2f + \dots \pmod{I} \\ &= a_1g_1 + a_2g_2 + \dots \pmod{I} \end{aligned}$$

Define

$$\tilde{f} = a_1g_1 + a_2g_2 + \dots$$

Note that for all i, j we have $\frac{g_j}{h_j} = f = \frac{g_i}{h_i}$ on the dense open sets $U_i \cap U_j$, so we see that $h_i g_j = h_j g_i$ on Y .
So:

$$\begin{aligned} h_i \tilde{f} &= a_1h_i g_1 + a_2h_i g_2 + \dots \\ &= a_1h_1 g_i + a_2h_2 g_i + \dots \\ &= g_i \pmod{I} \end{aligned}$$

So on U_i we have $\tilde{f} = \frac{g_i}{h_i}$, so $f = \tilde{f}$ is a polynomial. □

18.2.2 Regular functions on quasi-projective variety

Definition 18.8. U is **quasi-projective** if it is an open subset of a *projective* variety.

Any quasi-projective variety is covered by a finite number of open subsets of affine subvarieties, since projective space is covered by a finite number of copies affine space.

Definition 18.9. A function on a quasi-projective variety is **regular**, if it is **locally regular**. I.e. each point has a nbh that is an open subset of affine nbh where our function is regular (in the sense as in 18.7).

If Y is quasi-projective, for each open subset $U \subseteq Y$, we have a ring $\mathcal{O}(U)$ of regular functions.

Theorem 18. Suppose that Y is quasi-projective and $U \subseteq Y$, is open such that $U = U_1 \cup U_2 \cup \dots$, where U_i are open then:

- If $f \in \mathcal{O}(U)$ is such that $f = 0$ on $\mathcal{O}(U_i)$, then $f = 0$.
- If $f_i \in \mathcal{O}(U_i)$ and $f_i = f_j$ on $U_i \cap U_j$ then we can find $f \in \mathcal{O}(U)$ such that $f = f_i$ on U_i .

(We will see later that the regular function on open sets form what is called a **Sheaf of rings**)

Example 18.9.1. Find regular functions on \mathbb{P}^1 , we know that the regular functions on $\mathcal{A}^1 = k[x]$.

To specify a regular function on \mathbb{P}^1 , pick a regular function on \mathbb{A}^1 , i.e. $\in k[x]$ and another regular function on \mathbb{A}^1 , i.e. in $k[y] = k[x^{-1}]$ such that they are the same on $\mathbb{A}^1 \setminus 0$, i.e. in $k[x, x^{-1}]$.

But if $f \in k[x]$ and $g \in k[x^{-1}]$ is such that $f = g$ in $k[x, x^{-1}]$ this means that $f = \text{constant}$. All regular function on the projective line are constant.

18.2.3 Morphisms of varieties

We will now define what a morphisms of varieties is, and show how to make the category of varieties.

Say we have X, Y varieties, how do we define a “nice” function $f: X \rightarrow Y$? Well we know what a “nice” function $Y: k$ looks like, it is a regular function. The correct definition of f is such that the composition of f and a regular function is a regular function.

Definition 18.10. f is called a **morphism** if for any open $U \subseteq Y$, any regular $g: U \rightarrow k$, then $g \circ f$ is regular on $f^{-1}(U)$. (This is a morphism of **ringed spaces**, this is not the same a morphism of locally ringed spaces which we will define later)

The Quasi-projective varieties and morphisms form a **category**.

Definition 18.11. A **ringed space** is a topological space with a sheaf of rings.

I.e. with the properties listed in Theorem 18

Examples of Ringed Spaces:

- Topological spaces are ringed spaces, by taking continuous functions on open sets.
- C^1 manifolds, where differentiable functions with continuous derivatives.
- C^2 manifolds, where twice differentiable
- ...
- C^∞ (smooth) manifolds, ringed space given by taking all smooth functions.
- C^ω (analytic) manifolds
- Algebraic varieties over \mathbb{C} or \mathbb{R}

Algebraic varieties over \mathbb{C} or $\mathbb{R} \subseteq C^\omega \subseteq C^\infty \subseteq \dots \subseteq C^2 \subseteq C^1 \subseteq \text{Top space manifolds}$.

As we go in further in the chain in the direction of topological spaces, things get “floppier”, we can bend the manifolds very easily. Whilst algebraic varieties are very rigid, hard to bend. The division is made in between C^ω and C^∞ . Recall by analytical continuation if we define a function in one point, it is “automatically” defined near other points. The function is very rigid and we can’t modify it. But for smooth functions, we can make smooth function that are zero somewhere and non-zero somewhere else (bump functions) so we can bend the function quite easily.

So the category of algebraic varieties is very similar to the category of smooth or topological manifold. The main difference is that we have a different choice of rings, where the rings determine the function we are interested in.

Locally ringed spaces:

Definition 18.12. Local ring at a point $p \in X$, where X is a topological space with a sheaf of rings.

For each open set U of X we have a ring $\mathcal{O}(U)$, such that if $U \subseteq V$ we have a restriction map $\mathcal{O}(V) \rightarrow \mathcal{O}(U)$, the local ring at p is informally “functions defined near ” p .

More precisely, an element of the local ring is given by:

- An open set $U \ni p$
- A function $f \in \mathcal{O}(U)$

However $(f, U), (g, V)$ are considered to be the same if we can find $p \in W \subseteq U \cap V$ such that $f = g$ on W . The set of equivalence classes is a ring called the **local ring at p** .

All of our earlier examples (topological spaces, smooth manifolds, analytic manifolds) if we do this construction we get a local ring, it has a unique maximal ideal which is equal $\{\text{functions vanishing at } p\}$. In these cases we call the ringed space a **locally ringed space**.

Examples

Example 18.12.1. We take the hyperbola $xy = 1$ which is a subset of the plane an the line $\mathbb{A}^1 \setminus 0 \subseteq \mathbb{A}^1$.

Then the maps $(x, y) \rightarrow x$ and $x \rightarrow (x, x^{-1})$ are morphisms from the hyperbola to the $\mathbb{A}^1 \setminus 0$ and from $\mathbb{A}^1 \setminus 0$ to the hyperbola respectively. Furthermore these maps are inverses of eachother.

So these two objects are isomorphic in the category of quasi-projective varieties.

Example 18.12.2. Let us take the curve $y^2 = x^3$, there is a map from the affine line to this curve:

$$\begin{aligned}\mathbb{A}^1 &\rightarrow (y^2 = x^3) \\ t &\rightarrow (t^2, t^3)\end{aligned}$$

This is

1. continuous
2. Bijection
3. Homeomorphism
4. Morphisms of varieties
5. **NOT** an isomorphism of varieties

So even though this is a morphism of varieties and an isomorphism of the underlying topological space, this does not imply that this is an isomorphism of varieties. This is intuitive since $(y^2 = x^3)$ has a singularity but \mathbb{A}^1 does not. There is no way to define a regular map from this curve back to \mathbb{A}^1 , we can try $t = \frac{y}{x}$, but this is not regular at $x = 0$.

19 Affine algebraic sets and commutative rings

Relation between morphism of varieties and homomorphism of the corresponding coordinate rings.

Theorem 19. Suppose Y is affine, then morphisms from X to Y are “same as” homomorphisms of rings from $\mathcal{O}(Y)$ to $\mathcal{O}(X)$.

Note X can be any quasi-projective variety.

Proof. Suppose $\varphi \in \text{Mor}(X, Y)$. This means we have

$$X \xrightarrow{\varphi} Y \rightarrow \mathbb{A}^1$$

, so this gives us a homomorphism of rings $\text{Hom}(\mathcal{O}(X), \mathcal{O}(Y))$, where for $\psi \in \text{Mor}(Y, \mathbb{A}^1)$ we associate $\psi \circ \varphi$. This works for all Y .

Now we will construct a map from $\text{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$ to $\text{Mor}(X, Y)$. Suppose that $h \in \text{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$, note we can think of $\mathcal{O}(Y)$ as $k[x_1, \dots, x_n]/I$, since Y is affine $\subseteq \mathbb{A}^n$.

We construct $\psi: X \rightarrow Y$, note since $x_1, \dots, x_n \in k[x_1, \dots, x_n]/I = \mathcal{O}(Y)$ we can look at elements $h(x_i)$.

If $p \in X$, $(h(x_1)(p), \dots, h(x_n)(p)) \in k^n$, this defines a map $X \rightarrow \mathbb{A}^n = k^n$. We claim that this is ψ . **Exercise 1** We need to check:

1. The image is in Y , this follows from the fact that $h(I) = 0$
2. ψ is a morphism, this follows from $x_i \circ \psi$ is regular on X for each x_i
3. Need to check this is the inverse of the map φ .

□

Affine varieties over k are the “same as” finitely generated algebras over k with no nilpotents. So we don’t only get a one to one correspondence of the objects but also of the morphisms. “The same as” means that the first category is equivalent to the opposite of the second. (Note equivalent categories are hard to define precisely c.f. McLane category for the working mathematician; informally we can treat varieties as the same as fin gen algebras reversing the morph)

Consequences

Example 19.0.1. Products of varieties is equivalent to coproduct of algebras. Note a coproduct is a object $R \cup S$ such that these maps commute:

$$\begin{array}{ccc} C & \leftarrow & \\ \uparrow & \swarrow & \\ R \cup S & \xleftarrow{\quad} & R \\ \uparrow & & \\ S & & \end{array}$$

Recall in commutative rings the coproduct is just the tensor product. So the product of affine varieties corresponds to the tensor product of commutative rings.

Note this fails for over non-perfect fields. If K is an inseparable extension of k , then $K \otimes k$ may have NILPOTENT elements.

Definition 19.1. Algebraic group An algebraic group G , is an algebraic variety with morphisms:

- $G \times G \rightarrow G$, product
- $G \rightarrow G$, the inverse
- point $\rightarrow G$, identity

Where these maps follow the axioms of groups.

Example 19.1.1. G_a is the affine line \mathbb{A}^1 with $\mathbb{A}^1 \times \mathbb{A}^1 \rightarrow \mathbb{A}^1$ is $(x, y) \rightarrow x + y$.

The inverse is $x \rightarrow -x$, and the identity is 0.

Now from the point of view of rings:

$$k[x] \otimes k[y] \leftarrow k[z] \text{ where } z \rightarrow x + u$$

So we have two maps:

$$\begin{cases} k[x] \otimes k[y] \rightarrow k[z] & \text{ring multiplication} \\ k[x] \otimes k[y] \leftarrow k[z] & \text{Group operation} \end{cases}$$

These maps are in some sense duals of each other, this is **Cartier Duality**.

Example 19.1.2.

$$\begin{aligned} G_m: \mathbb{A}^1 \setminus 0 \quad (x, y) &\rightarrow xy \\ k[x, x^{-1}] &\rightarrow k[x, x^{-1}] \otimes k[x, x^{-1}] \text{ by } x \rightarrow x \otimes x \end{aligned}$$

Example 19.1.3.

$$\begin{aligned} GL_2(k): \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} &= \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \end{aligned}$$

What is the coordinate ring?

$$R = k[a, b, c, d, (ad - bc)^{-1}] = k[a, b, c, d, l]/((ad - bc)l = 1)$$

With product

$$\begin{aligned} R &\rightarrow R \otimes R \\ a &\rightarrow a_1a_2 + b_1c_2 \\ b &\rightarrow a_1b_2 + b_1d_2 \\ c &\rightarrow c_1a_2 + d_1c_2 \\ d &\rightarrow c_1b_2 + d_1d_2 \end{aligned}$$

The inverse

$$\begin{aligned} R &\rightarrow R \\ a &\rightarrow \frac{d}{ad - bc} \\ b &\rightarrow \frac{-b}{ad - bc} \\ &\vdots \end{aligned}$$

The coordinate rings of affine alg groups like this are called **Hopf Algebras**.

The twisted cubic We will show that the twisted cubic is isomorphic to \mathbb{P}^1 . Recall that the twisted cubic is

$$(w: x: y: z) = (s^3: s^2t: st^2: t^3) \in \mathbb{P}^3$$

Equivalently it can be described as

$$\text{the vanishing of } \{wy - x^2, xz - y^2, wz - xy\}$$

So the coordinate ring is given by $k[w: x: y: z]/(wy - x^2, xz - y^2, wz - xy)$.

First of all there is an obvious map from $\mathbb{P}^1 \rightarrow$ twisted cubic:

$$(s: t) \rightarrow (s^3: s^2t: st^2: t^3)$$

This is an isomorphism of topological space, but this doesn't imply that this is an isomorphism of varieties.

We need to find a regular map: Twisted cubic $\rightarrow \mathbb{P}^1$. To do this we will cover the cubic by open affine sets U_i and choose functions on each U_i , and check they are the same on $U_i \cap U_j$.

Recall that \mathbb{P}^3 is covered by four copies of \mathbb{A}^3 , the twisted cubic is covered by two affine sets $w \neq 0$ and $z \neq 0$. Indeed from the definition we see that $w = z = 0$, then $x = y = 0$.

So we have maps:

$$\begin{aligned} w \neq 0: (w: x: y: z) &\rightarrow (w: x) \in \mathbb{P}^1 \\ w \neq 0: (w: x: y: z) &\rightarrow (y: z) \in \mathbb{P}^1 \end{aligned}$$

Furthermore these maps are compatible, on the intersection $w \neq 0, z \neq 0$ since $wz = xy$ on the cubic we see $(w: x) = (y: z)$. So we have a morphism from the cubic to \mathbb{P}^1 , it is straightforward to see that this is the inverse of the map above.

Recall two affine varieties are isomorphic if and only if their corresponding coordinate ring are isomorphic. Is this true for projective varieties? No!

If we look at \mathbb{P}^1 its corresponding graded ring is $k[x, y]$ where $\deg x = \deg y = 1$. On the cubic the corresponding graded ring is $k[w, x, y, z]/(wy - x^2, xz - y^2, wz - xy)$ with $\deg x, y, z, w = 1$

These two rings are NOT isomorphic. In degree 1, the first ring is 2 dimensional but the second one is 4 dimensional.

$\mathbb{A}^2 \setminus (0,0)$ is NOT affine We will show this space is not affine by calculating the ring of regular functions on it. In order to do this we will cover $\mathbb{A}^2 \setminus (0,0)$ by two affine sets U, V ,

We let $U = \mathbb{A}^2 \setminus$ x-axis and $V = \mathbb{A}^2 \setminus$ y-axis, their coordinate rings are $k[x, y, y^{-1}]$ and $k[x, y, x^{-1}]$ respectively. The coordinate ring of the intersection has coordinate ring $k[x, y, x^{-1}, y^{-1}]$.

So we are looking for functions on $k[x, y, x^{-1}, y^{-1}]$ that can be expressed as polynomials in $k[x, y, x^{-1}]$ and $k[x, y, y^{-1}]$. These are nothing but the polynomials in $k[x, y]$.

So the regular function on $\mathbb{A}^2 \setminus (0,0)$ are $k[x, y]$. Now notice since we have a morphism $\mathbb{A}^2 \setminus (0,0) \rightarrow \mathbb{A}^2$, we have the corresponding homomorphism from the coordinate rings: $k[x, y] \hookrightarrow k[x, y]$.

Since morphism of affine varieties correspond exactly to homomorphism of coordinate ring, if $\mathbb{A}^2 \setminus (0,0)$ where affine then since $k[x, y] \hookrightarrow k[x, y]$ is an isomorphism then $\mathbb{A}^2 \setminus (0,0) \simeq \mathbb{A}^2$, but this is not possible. So $\mathbb{A}^2 \setminus (0,0)$ is NOT AFFINE.

Note that \mathbb{A}^1 is affine, since in general if we remove a subset that is codimension 1 from an affine variety it remains affine, but if we remove a subset of codimension 2 (like for $\mathbb{A}^2 \setminus (0,0)$) or more it quite often no longer affine. **analogue in complex analysis:** functions can't have zeros that are of codimension 2 or more.

More examples We want to show that the *product* of two algebraic varieties is also an algebraic variety. To show this we just need to show that the product of two projective space is a projective variety.

Recall the Segre embedding:

$$\mathbb{P}^m \times \mathbb{P}^n \rightarrow \mathbb{P}^{mn+m+n} \text{ given by } ((x_0: \dots : x_m), (y_0: \dots : y_n)) \rightarrow (x_0y_0: x_0y_1: \dots : x_my_n) = (z_{00}: z_{01} \dots)$$

We want to show that the image of this embedding is a product in the category of varieties.

We just need to show that the image of the Segre embedding maps to \mathbb{P}^m and \mathbb{P}^n and is universal with this property. If $z_{00} \neq 0$, we have a map:

$$\begin{aligned} (\text{SEGREG}) &\rightarrow \mathbb{P}^m \\ (z_{00}: z_{01}: \dots) &\rightarrow (z_{00}: z_{10}: z_{20} \dots) \in \mathbb{P}^m \end{aligned}$$

If $z_{01} \neq 0$:

$$\begin{aligned} (\text{SEGREG}) &\rightarrow \mathbb{P}^m \\ (z_{00}: z_{01}: \dots) &\rightarrow (z_{01}: z_{11}: z_{21} \dots) \in \mathbb{P}^m \end{aligned}$$

Do these maps coincide on the intersection of the open sets? Yes it follows from the fact that $z_{ij}z_{kl} = z_{il}z_{kj}$, we have that:

$$\begin{aligned} (z_{00}: z_{10}: z_{20} \dots) &= (z_{01}z_{00}: z_{01}z_{10}: z_{01}z_{20} \dots) \text{ since } z_{01} \neq 0 \\ &= (z_{01}z_{00}: z_{11}z_{00}: z_{21}z_{00} \dots) \\ &= (z_{01}: z_{11}: z_{21} \dots) \end{aligned}$$

. Similarly for the other open subsets covering the SEGREG variety we can check that we get a well defined map as above on \mathbb{P}^m and they are the same on the intersection.

Now assume we have any other variety C mapping to \mathbb{P}^m and \mathbb{P}^n . Since we can cover C by open affine varieties, if we show that each of these open subsets give us a map to SEGREG, since they must coincide in their intersections by uniqueness of map of product, it will give us a map from C to SEGREG.

So we can assume that C is affine.

$$C \xrightarrow{\text{morphism}} \text{open subset } x_0 \neq 0 \text{ at } \mathbb{P}^m$$

Is given by $(\underbrace{f_0, f_1, \dots, f_m}_{\parallel 1})$ where the f_i are regular on C .

Likewise for $y_0 \neq 0 \in \mathbb{P}^n$, we have

$$(\underbrace{g_0, g_1, \dots, g_n}_{\parallel 1})$$

So we get a map from C to SEGREG by $C \rightarrow (f_0g_0: f_0g_1: \dots : f_ng_n)$

19.1 Automorphism of space

In general the group of automorphism of an algebraic set is the trivial group, however affine space and projective space are very symmetrical and have a lot of automorphisms.

Automorphism of affine space First of all we look at \mathbb{A}^1 , recall its coordinate ring is $k[x]$, so morphisms of $\mathbb{A}^1 \rightarrow \mathbb{A}^1$ correspond to

$$\begin{aligned} k[x] &\rightarrow k[x] \\ x &\mapsto p(x), \text{ for some polynomial} \end{aligned}$$

This is invertible iff $p(x) = ax + b$ for $a \neq 0$. We call the group of automorphism the “ $ax + b$ group” for this reason. We can identify it with the group:

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

Properties:

1. This group is noncommutative
2. It has got a normal subgroup, consisting of the elements of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \simeq k$, the quotient is isomorphic to k^*

This group is a counterexample to a lot of things.

Now what about \mathbb{A}^2 ? Some obvious automorphisms are:

$$\begin{aligned} k[x, y] &\rightarrow k[x, y] \\ x &\rightarrow ax + by + c \\ y &\rightarrow dx + ey + f \end{aligned}$$

Where $\det \begin{pmatrix} a & b \\ d & e \end{pmatrix} \neq 0$

The set of elements of this form does give us a group of automorphism, but it is not the full group. The full group of automorphisms is much bigger.

For example we have the following automorphism:

$$\begin{array}{ll} x \rightarrow x; & x \rightarrow x \\ & \text{inverse} \\ y \rightarrow y + p(x); & y \rightarrow y - p(x) \end{array}$$

For some polynomial $p(x)$. This give us an infinite dimensional abelian subgroup.

Suppose we have an automorphism of \mathbb{A}^n where we map $x_i \rightarrow f_i(x_1, \dots, x_n)$, when is this an automorphism? If we look at the Jacobian, $\det(\frac{\partial f_i}{\partial x_j})$.

The Jacobian of FG is the Jacobian of F times the Jacobian of G , so if $FG = 1$ then Jacobian of F is invertible. So we can conjecture that our map is an automorphism of affine space if and only if the jacobian is invertible.

Jacobian Conjecture: If the Jacobian of F is invertible then F is an automorphisms. This is still a very difficult open problem.

Morphisms of projective space We will start looking at \mathbb{P}^1 .

If we have a map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$, we can restrict it to a map from $\mathbb{A}^1 \rightarrow \mathbb{A}^1$. This gives us a map:

$$\underbrace{\text{open subset } \mathbb{A}^1 \rightarrow \mathbb{A}^1}_{\text{rational function } \frac{p(x)}{q(x)}} \subseteq \mathbb{P}^1$$

Since $\mathbb{P}^1 = \mathbb{A}^1 \cup \infty$.

Conversely given a rational function from an open subset of \mathbb{A}^1 to \mathbb{A}^1 can be extended to a map from \mathbb{P}^1 to \mathbb{P}^1 .

So this gives us all the morphisms of \mathbb{P}^1 to itself, which of these maps have inverses? Those of the form $\frac{ax+b}{cx+d}$, where $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$

$$GL_2(k) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \det \neq 0 \right.$$

This almost gives us the group of automorphism we need to quotient out by the diagonal matrices since

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \text{ which corresponds to the map } x \rightarrow \frac{ax}{a} = x$$

So the group of automorphisms is:

$$\mathbb{P}GL_2(k) = GL_2(k) / \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right)$$

This is the projective general linear group, it is of dimension $4 - 1 = 3$ and contains the $ax + b$ group as a subgroup.

Recall the Riemann sphere from complex analysis, the endomorphisms of the projective line are the same as the endomorphisms of Riemann space. However the group of endomorphisms of the complex plane is the group of entire functions which is much bigger than the group of endomorphisms of the affine line, which is only the group of polynomials.

For the projective line algebraic geometry is very similar to doing this analytically, whereas in the affine line it is different. C.f. **SERRE: Géométrie Analytique et Géométrie Algébrique**, roughly speaking it says that working over projective manifolds, then analytic maps tend to be algebraic. But if we are working with affine manifolds analytic things are much more common than algebraic things and quite often not algebraic.

Affine plane We look at at the map

$$\begin{array}{ccc} \mathbb{A}^2 & \rightarrow & \mathbb{A}^2 \\ (x, y) & \rightarrow & (x, xy) \end{array}$$

What is the image of this? It is $\{(x, y) \mid x \neq 0\} \cup \{(0, 0)\}$, the image is not open, closed or even locally closed!

20 The Ax Grothendieck theorem

Definition 20.1. A **first order** statement is a statement that can be written in first order logic with these logical connectives:

$$\wedge(\text{and}), \vee(\text{or}), \neg(\text{not}), \rightarrow(\text{implies.})$$

And with the operators of our field:

$$a + b, a \cdot b, a - b$$

And we are allowed to quantify over all elements we are working on:

$$\forall x \in X, \exists x \in X$$

Example 20.1.1. To say a field is algebraically closed, we mean for all polynomials $a_n x^n + \dots$, there exists a root, but this is a wrong statement in first order logic since we can't say *for all polynomials*, we can only talk about elements in our field.

We can say for all polynomials of degree n , $a_n x^n + \dots$ since this is equivalent to saying for all $a_n, a_{n-1}, \dots, a_0 \dots$

So in order to say that X is algebraically closed we need to take an infinite statements of first order logic.

Theorem 20. *The Theory of alg closed field of a given characteristic p , is **COMPLETE** (everything is provable or disprovable).*

Proof. There is a unique algebraically closed field of a given characteristic and cardinality c . From theorem of first order logic we know that if there is a unique model of some theory in some characteristic then that theory is complete. (c,f, Gödel's completeness theorem). \square

From this we can say that anything true for algebraically closed fields of large characteristic is true for algebraically closed fields of characteristic zero.

How do we say something is a field of characteristic zero? We can't say this with first order logic with finite number of statements, we need to say $2x \neq 0, 3x \neq 0, 5x \neq 0, \dots$

So suppose we prove something about algebraically closed fields of characteristic zero, every proof uses a finite number of axioms. If we proved something about algebraically closed fields of characteristic zero, it is true for all closed fields of sufficiently large characteristic, since our proof can only eliminate a finite number of characteristics (the $2x \neq 0$, etc... statements).

Conversely if something is true for all algebraically closed fields in large characteristics it is also true for characteristic fields in characteristic 0. This implies the following theorem:

Ax Grothendieck Theorem

Theorem 21. *Let V be an algebraic variety. If we have a regular map $f: V \rightarrow V$ over an algebraically closed field k , if f is injective it is surjective,*

Counter-example

- If k is not algebraically closed this theorem is false, for example take $k = \mathbb{Q}$ and $f(x) = x^3$.
- If $k = \mathbb{C}$ we can take $f(x) = x^2$, this map is surjective but not injective.

Proof. This theorem is trivial if k is finite. It is also true over any algebraic extension of a finite field (the coeffs of all equations defining a variety and the coeffs of a point, all lie in some finite field). So we if we have an injective map over an algebraic extension if we have to show it is surjective take a finite extension of the finite field containing a certain point, and apply the finite case.)

Since this is true for all algebraic extensions of a finite field it is true for all algebraically closed fields. It is true for all algebraic closures of finite fields, a result from model theory tells us that a (first order) statement is true for all closed fields in char 0 if and only if it is true for all closed fields of all sufficiently large characteristic.

A second result from logic says that if a (first order) statement is true for one algebraically closed field of a given characteristic it is true for all. This is the Lefschetz principle. \square

For other proofs where we prove something in characteristic p in order to get a statement in characteristic zero, cf Mori's Bend or Break argument.

Lecture 5: Rational maps

We will now start the lecture on **Rational maps**

21 Rational functions and rational maps

Definition 21.1. Suppose Y is an affine variety, then $\mathcal{O}(Y)$ is an integral domain. We can form the quotient field $K(Y)$, we call these **rational functions**(on Y).

For example if $Y = \mathbb{A}^2$, then $\mathcal{O}(Y) = k[x, y]$, so $K(Y) = k(x, y)$, i.e. the elements of the form $\frac{p(x, y)}{q(x, y)}$, where $q(x, y) \neq 0$.

Recall regular functions on affine varieties correspond to holomorphic functions for Riemann surface. Whereas rational functions correspond to meromorphic functions (the field of quotient of holomorphic functions).

Example with projective variety If Y is a projective variety, we can't do the previous construction since the ring of regular functions on Y is k . So the field of quotients is k , which is not interesting.

So we need to define rational functions on projective variety in a different way.

Definition 21.2. **Rational function** is given by:

- (a) Dense (affine) open set U .
- (b) Rational function on U .

Suppose we have two rational functions (f_1, U_1) and (f_2, U_2) they are identified if $f_1 = f_2$ on a dense open set contained in U_1 and U_2 .

The rational functions are given by taking a direct limit over dense open affine sets U of $K(U)$.

It is not difficult to check that the rational functions on $K(Y)$ form a field (note we take Y to be an irreducible variety).

21.1 Rational maps between varieties

Suppose X, Y are varieties. A rational map $X \rightarrow Y$ is a regular map $U \rightarrow Y$, where U is dense and open in X . We identify two of these maps in the obvious way. $(f_1, U_1) = (f_2, U_2)$ if $f_1 = f_2$ on $U \subseteq U_1 \cap U_2$, where U is dense and open.

Rational maps $X \rightarrow \mathbb{A}^1$ are rational functions on X .

Unfortunately rational maps do not form a category, since composition is not defined. Taking the rational maps:

$$\mathbb{A}^1 \xrightarrow{0} \mathbb{A}^1 \xrightarrow{x \mapsto \frac{1}{x}} \mathbb{A}^1$$

The image of the first map is 0, but the domain of the second map does not contain zero, so composition is not defined.

Definition 21.3. A rational map is said to be **dominant**, if its image contains a dense open set.

If we restrict ourselves to dominant rational maps then composition is well-defined.

Birational

Definition 21.4. We say X, Y are **birational** if we got rational maps from $X \rightarrow Y$ and $Y \rightarrow X$, whose composition is equal to the identity on a dense open subset.

So isomomorphic maps are birational, but not all birational map is isomorphic.

Example 21.4.1. Take varieties $\mathbb{A}^1, \mathbb{P}^1, xy = 1, x^3 = y^2$.

We have seen earlier that these four varieties are all birational to each other. \mathbb{A}^1 is \mathbb{P}^1 minus a point, $xy = 1$ is identified to \mathbb{A}^1 minus a point, and there is a map from \mathbb{A}^1 onto $x^3 = y^2$ which is an isomorphism onto \mathbb{A}^1 minus a point.

However no two of these varieties are equivalent. For example the curve defined by $x^3 = y^2$ has some sort of singularity, etc...

Example 21.4.2. Two dimensional example $\mathbb{P}^1 \times \mathbb{P}^1, \mathbb{P}^2, \mathbb{A}^2, \mathbb{A}^2 \setminus (0, 0)$.

These are all birational to \mathbb{A}^2 , but no two of these are isomorphic.

Definition 21.5. Varieties that are birational to an affine space are called **rational varieties**.

Are there non-rational varieties? Yes.

Example 21.5.1. Fermat's Last theorem for polynomials $x^3 + y^3 = 1$ is not birational to \mathbb{A}^1 . More generally there is no dominant rational map from the affine line onto this curve.

Assume we had a map from \mathbb{A}^1 to this curve which is dominant (so non-constant). This means we have

$$x(t)^2 + y(t)^2 = 1, \text{ where } x, y \text{ rational functions}$$

By clearing denominators we can find f, g, h polynomials such that:

$$f(t)^3 + g(t)^3 = h(t)^3$$

We can assume they are coprime, and let's work over \mathbb{C} to factor them:

$$\underbrace{(f(t) + g(t))}_{\text{cube, we call } h_1^3} \underbrace{(f(t) + \omega g(t))}_{\text{cube, we call } h_2^3} \underbrace{(f(t) + \omega^2 g(t))}_{\text{cube, we call } h_3^3} = h(t)^3 \text{ note } K[t] \text{ form a UFD}$$

Remark. We can use Bézout or something similar to show that $f(t) + g(t)$, $f(t) + \omega g(t)$ and $f(t) + \omega^2 g(t)$ are coprime. Which is why we know they are cubes, since the product of coprime polynomials is a cube iff they are each a cube.

So we get three equations: $f + g = h_1^3$, $f + \omega g = h_2^3$, $f + \omega^2 g = h_3^3$. We can eliminate f, g and get a linear relation between h_1^3, h_2^3, h_3^3 . If we multiply h_i by constants we get another relation of polynomial that says:

$$h'_1^3 + h'_2^3 = h'_3^3 \text{ where } h'_i = a_i h_i, a_i \in \mathbb{C}$$

So if f, g and h are not constant, then h'_1, h'_2, h'_3 are non-constant have smaller degree than f, g and h . So for any solution of this equation we get a solution of smaller degree. \perp

Note this works for any exponent that is at least 3, the result is false for exponent two though, since for example we have:

$$(1 - t^2)^2 + (2t)^2 = (1 + t^2)^2$$

This comes from the fact that $x^2 + y^2 = 1$ IS rational as was seen in lecture 1.

The reason we can't replicate our previous proof is that we can't create a relation between h_1, h_2, h_3 as we did above. We end up with

$$(t^2 + 1)^2 = \underbrace{(t+i)^2}_{h_1} \underbrace{(t-i)^2}_{h_2}$$

Fermat's Last theorem for polynomials is almost trivial, we have just done it. Whereas for the integers it is incredibly difficult. The reason for the difference is that polynomials over a field are "nicer" than the cyclotomic field we need to use for the integer case. In particular polynomials over a field form a UFD and all units are nth powers for any n.

22 Elliptic functions and cubic curves

Definition 22.1. An **elliptic function** is a meromorphic function such that:

$$f(z + \lambda) = f(z)$$

For all $\lambda \in L$, where L is a lattice in \mathbb{C} , i.e. there are $a, b \in \mathbb{C}$ such that $L = \{na + mb \mid n, m \in \mathbb{Z}\}$.

Note if f is holomorphic it will be bounded so constant by Liouville. So if f is non-constant it must have poles.

How can find functions with this property? One way is take a function g and define:

$$f(z) = \sum_{\lambda \in L} g(z + \lambda)$$

Note the function g we need to choose must be chosen so that this sum converges. For example $g(z) = \frac{1}{z}$ doesn't converge, so we can't use it. If we take $g(z) = \frac{1}{z^3}$, it converges well. If we take $g(z) = \frac{1}{z^2}$ it is "borderline", it doesn't converge but if we modify it slightly it does converge.

Definition 22.2. The Weierstrass P-function:

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z - \lambda)^2} - \underbrace{\frac{1}{\lambda^2}}_{\text{constant}} \right)$$

Note we can show that $\wp'(z)$ is doubly periodic so \wp is doubly periodic up to a constant. So

$$\wp(z + a) = \wp(z) + \text{constant}$$

This constant is zero since \wp is an even function.

Laurent expansion at z=0

$$\wp(z) = \frac{1}{z^2} + 0z + *z^2 + \dots$$

So for the derivative:

$$\wp'(z) = -2z^{-3} + *z + \dots$$

$$\begin{aligned}\wp'(z)^2 &= 4z^{-6} + *z^{-2} + *z^0 + \dots \\ 4\wp(z)^3 &= 4z^{-6} + *z^{-2} + \dots\end{aligned}$$

So we can see that:

$$\underbrace{\wp'(z)^2}_{\text{doubly periodic, no poles, vanishes at } z=0} = 4\wp(z)^3 + *\wp(z) + * + O(z)$$

Since it is doubly periodic, and has no poles it is constant but since it vanishes at 0, it must be zero. So the Weierstrass p function satisfies the following differential equation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp - g_3$$

Why are these things called elliptic functions? Since if we take the arc length of an ellipse we get what is called an **elliptic integral**:

$$\int \frac{dx}{\sqrt{4x^3 - ax - b}}$$

We find that the Weierstrass p function is some sort of inverse:

$$z = \int \frac{d\wp}{\sqrt{4\wp^3 - g_2\wp - g_3}}$$

The inverses of elliptic integrals are doubly periodic, so doubly periodic are called elliptic functions.

Back to algebraic geometry Let us look at the equation:

$$y^2 = 4x^3 - g_2x - g_3$$

If we take $y = \wp'(z)$ and $x = \wp(z)$, then (x, y) lies on the curve. So we have a map from $\mathbb{C} \setminus L$ onto the curve $y^2 = 4x^3 - g_2x - g_3$ taking $z \rightarrow (\wp'(z), \wp(z))$.

We can extend this a function from \mathbb{C} to the projective curve by mapping the point 0 to the point at infinity.

But since the map is doubly periodic we get a homeomorphism of topological spaces:

$$S^1 \times S^1 \simeq \mathbb{C}/L \rightarrow \text{PROJECTIVE CURVE}$$

So this curve with a point added at infinity is homeomorphic to the two-dimensional torus, so this can't be rational. Since any rational curve is the same as \mathbb{P}^1 up to a finite number of points. And $\mathbb{P}^1 \simeq S^2$, there is no way to turn a torus into a sphere by adding and removing a finite number of points.

If we have a rational map between \mathbb{P}^1 and our curve, it will be defined except at a finite number of points, and would have an inverse that is well-defined except at a finite number of points. So any two birational curves are the same topologically, so these two curves can't be birational.

Singly periodic functions We can take the non absolutely convergent sum $\sum \frac{1}{z-\lambda}$, and make it converge by summing it over λ by order of absolute value and this a periodic function equal to

$$\pi \cot(\pi z)$$

This gives rise to the product formula of the sin function:

$$\sin(\pi z) = z \prod_{n \neq 0} \left(1 - \frac{z}{n}\right)$$

Taking the log derivative on both sides we get the above identity.

23 Rationality of cubic surfaces

Recall that for cubic curves, for example of the form $x^3 + y^3 + z^3 = 0$ in \mathbb{P}^2 are not rational. If we look at a cubic surface, $w^3 + x^3 + y^3 + z^3 = 0$ in \mathbb{P}^3 , we may think it is not rational but it is!

Informal argument to show that cubic surfaces are rational.

If we take two non-intersecting lines:

$$\begin{aligned} w+x=0, y+z=0 \\ w+y=0, x+\zeta z=0, \text{ where } \zeta^3=1 \end{aligned} \tag{\dagger}$$

These lines don't intersect, recall the point $(0:0:0:0)$ is not in \mathbb{P}^3 .

If we take a point on each of these lines and draw the line through the two points, the line will generally intersect the cubic surface at three points (so two points on each line and a third point on the surface). There is a problem, it is possible that the line lies entirely on the cubic surface. But let us ignore that for now.

What this is giving us a point x on a copy of \mathbb{P}^1 and y on another copy of \mathbb{P}^1 and we get a point on the cubic surface. $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow$ cubic surface.

This map is not defined everywhere, since if x, y happen to lie on a line that lies entirely on the cubic surface the third point is not defined. So this map is not defined everywhere and is in fact a rational map.

Does this map have a rational inverse? Suppose we have a point, that lies on two different lines, i.e. we have two different (x, y) and (w, z) such that our point is on the line intersecting x, y and w, z . These two lines form a plane which contain our lines \dagger , which mean they intersect which is a contradiction.

This strongly suggest that this map is map is 1 to 1 and has a rational inverse, so we can see show that in any cubic surface of two non-intersecting lines is birational to $\mathbb{P}^1 \times \mathbb{P}^1$.

Different argument for why most cubic surfaces are non-rational Pick 6 points in \mathbb{P}^2 , in **general position**. Points in general position, are points that don't satisfy a number of special conditions:

- No three are on a line
- Not all on a conic

We will look at the space of all cubic functions. This space is ten dimensional, and we look at the cubics vanishing on all six points. This gives us six linear relation on a ten dimensional space, this gives us a four dimensional space spanned by f_1, f_2, f_3, f_4 .

If we try to define the map $(x: y: z) \rightarrow (f_1: f_2: f_3: f_4)$, then this map is well-defined everywhere except at six points, where all these four functions vanish.

What is the image of this map from \mathbb{P}^2 to \mathbb{P}^3 ? Let's assume it is a hypersurface, what is its degree? We work it out by counting the number of intersection points with the line.

Pick a line in \mathbb{P}^3 , say $f_1 = f_2 = 0$. By Bézout's theorem which we will prove later, we can show that these have nine intersection points. Six of these are the six points we started with, which don't really count since their images aren't in \mathbb{P}^3 .

So this leaves us with three points, so the hypersurface has degree 3.

The dimension of the space of cubics is 19 and so is the dimension of the space of cubic surfaces obtained by taking six points. (We see this with an argument based on the dimensions of aut groups). So we can assume that we get all cubic surfaces in this way.

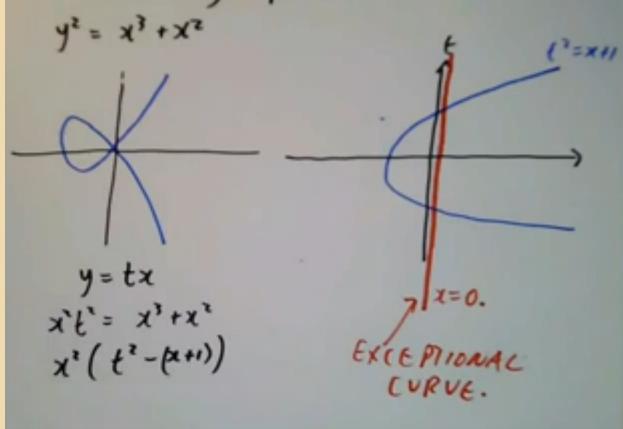
Everything we did here is a bit wishy-washy, this is typical of old style algebraic geometry arguments. The arguments are quite short and generally give the right answer, but every now and then they give a hopelessly **wrong** answer. While this is not a proof the result is correct, we need to do more work to show this rigorously.

24 Blowing up a point

Suppose we take the curve $y^2 = x^3 + x^2$, it has a singularity at the origin. We simplify it by making the substitution $y = tx$. This gives us

$$\begin{aligned} x^2 t^2 &= x^3 + x^2 \\ x^2(t^2 - (x+1)) &= 0 \end{aligned}$$

So in the $x - t$ plane, we get two curves, the curve $t^2 = x + 1$ and the curve $x = 0$. So our original curve has been transformed into a curve without singular points, except we pick up a new line called the exceptional curve.



So this point in the plane is replaced by the red line, which contains a point for each direction going through the origin; but it doesn't include a point for the vertical line going through the origin. So blowing up includes one extra point.

General form for blowing up at a point Suppose we have a general plane \mathbb{A}^2 and we blow it up at the point $(0,0)$. To do this include two new variables, $(X: Y) \in \mathbb{P}^1$.

Now look at the variety

$$\begin{aligned} &\mathbb{A}^2 \times \mathbb{P}^2 \\ &x, y, X: Y \end{aligned}$$

And we look at the subset of this such that $xY = yX$. If $(x, y) \neq (0, 0)$, there is just one point of \mathbb{P}^1 corresponding to it. Otherwise if $(x, y) = (0, 0)$ then we get the whole affine line \mathbb{P}^1 .

Definition 24.1. The subset of $\mathbb{A}^2 \times \mathbb{P}^2$ defined by this is called the **blow up** of \mathbb{A}^2 at a point.

So we have a map:

$$\begin{aligned} \text{Blow up} &\rightarrow \mathbb{A}^2 \\ x, y, X: Y &\rightarrow (x, y) \end{aligned}$$

And the Point $(0, 0) \Rightarrow \mathbb{P}^1$.

Recall \mathbb{P}^1 is defined by the two affine lines:

- $X \neq 0$, i.e. $X = 1$. In this case $xY = y$
- $Y \neq 0$, i.e. $Y = 1$. In this case $x = yX$

Definition 24.2. In n dimensions this is similar. Take \mathbb{A}^n , given by (x_1, \dots, x_n) and \mathbb{P}^{n-1} given by $(X_1: \dots: X_n)$ and look at:

$$\text{the subset of } \mathbb{A}^n \times \mathbb{P}^n \text{ given at } x_i X_j = x_j X_i \forall i, j$$

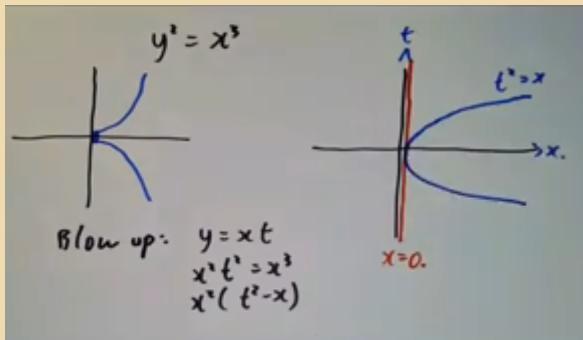
The subvariety defined by all these points maps to \mathbb{A}^n , the inverse image of

$$(x_1, \dots, x_n) = \begin{cases} \text{point, if } x \neq (0, \dots, 0) \\ \mathbb{P}^{n-1} \text{ otherwise} \end{cases}$$

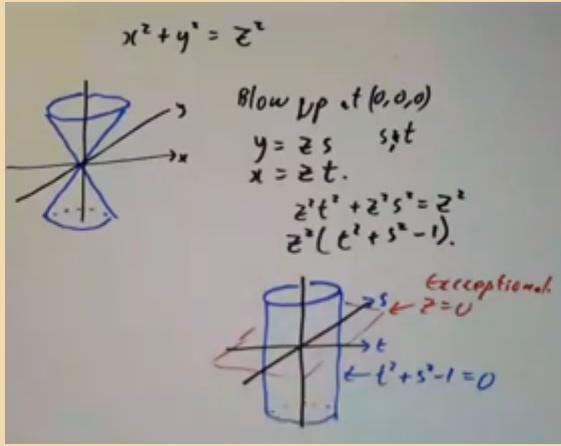
Now if $X_1 = 1$ we have $x_i = x_1 X_i \Rightarrow X_i = \frac{x_i}{x_1}$.

24.1 Application of Blow up: Resolving singularities

We look at the point $y^2 = x^3$, it has a singularity at the origin. Let us look at the blow up at the origin:



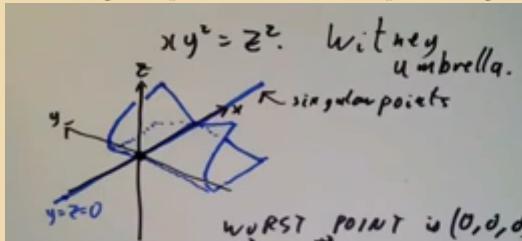
24.1.1 Higher dimensions:



Another example is the curve $y^8 = z^5$:

- Blow up: $z = yt$, we get $y^5(t^5 - y^3) = 0$. But $(t^5 - y^3)$ also has a singularity;
- Blow up: $y = ts$, then $t^3(s^3 - t^2) = 0$; another singularity;
- Blow up: $t = su$, so $s^3 = s^2u^2 \Rightarrow s = 0$ or $s = u^2$, so finally we have transformed our curve into a curve without a singularity.

Withney umbrella We look at the set $xy^2 = z^2$. It gives us a plane that sort of folds in on itself, with the axis $y = z = 0$ a line of singular points. The worst point is given at $(0,0,0)$. So let's blow it up.



Take $y = xY$ and $z = xZ$ we get:

$$x(x^2Y) = x^2Z^2 \Rightarrow x^2(xY^2 - Z^2) = 0$$

Which gives us the same singular point. So what can we do? We can try to blow it up along a line.

Take:

$$\begin{array}{ccc} \mathbb{A}^2 & \times & \mathbb{P}^2 \\ (x, y, z) & \times & (s: t) \quad yt = zs \end{array}$$

So, choosing $s = 1$ we get:

$$\begin{aligned} xy^2 = z^2 &\Rightarrow xy^2 = y^2t^2 \\ &\Rightarrow y^2 = 0 \text{ or } x = t^2 \end{aligned}$$

24.2 More on blow ups

What happens if we blow up a point on \mathbb{R}^2 ? Let's blow up the origin:

We take the set of all points

$$\{((x, y), (s: t)) \mid xt = ys\} \subseteq \mathbb{R}^2 \times \mathbb{P}^1$$

The point $(0, 0)$ corresponds to \mathbb{P}^1 over the reals which is just the circle S^1 . So we can think of this as having a point for each possible directions through the origin.

So we have a map

$$\begin{aligned} E = \text{Blow up} &\rightarrow \mathbb{P}^1(\mathbb{R}) = S^1 \\ (x, y), (s: t) &\rightarrow s: t \end{aligned}$$

The inverse image of $(s: t)$ is \mathbb{R} . So we have a map from E to S^1 such that the fibres are \mathbb{R} . We may think E corresponds to the cylinder but that is wrong, since the blowup is non-orientable. So E is homeomorphic to an open Moebius band.

This is surprising, we started with an orientable surface and blowing it up at a point gave us a non-orientable surface.

Next example Let's try to construct a map from $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^2$.

$$(x_0: x_1), (y_0: y_1) \rightarrow (x_0y_0: x_1y_0: x_0y_1) \text{ not defined at } x_0 = y_0 = 0$$

So this is defined everywhere except at a point $(0: 1) \times (0: 1)$. Let's fix this with blow ups.

Blow up $\mathbb{P}^1 \times \mathbb{P}^1$ at $(0: 1) \times (0: 1)$.

Cover with a copy of \mathbb{A}^2 given by the points where $x_1 = 1$ and $y_1 = 1$ (so the affine plane is (x_0, y_0)). If we blow this up at $x_0 = y_0 = 0$ by putting:

$$\begin{aligned} x_0 &= ty_0 \\ \Rightarrow (x_0y_0: x_1y_0: x_0y_1) &\\ \Rightarrow (ty_0^2: x_1y_0: ty_0y_1) &\\ \Rightarrow (ty_0: x_1: ty_1) &\in \mathbb{P} \end{aligned}$$

We've started with a rational map, and we found that if we blow up on point we get a regular map. Is this an isomorphism? No! If we look at $(0: 0: 1) \in \mathbb{P}^2$ this is the image of the line in $\mathbb{P}^1 \times \mathbb{P}^1$.

This is the image of the line where $y_0 = 0$.

Likewise the point $(0: 1: 0)$ is the image of the line $x_0 = 0$.

We can show that this map from the blowup to \mathbb{P}^2 is the same as the map if we blow up these two points of \mathbb{P}^2 . So the blow up of $\mathbb{P}^1 \times \mathbb{P}^1$ at one point is equal to the Blow up of \mathbb{P}^2 at two points.

More generally: There is several other things we can do with blowups

Blow up	Geometric meaning
Point p	$p \rightarrow \mathbb{P}$ (the tangent space of p)
Subvariety X	$p \in X \rightarrow \mathbb{P}$ (normal space at p)
Ideal	
“Quasicoherent sheaf of graded algebras”	Projective space of graded algebra at each point

Remark. What is a quasicoherent sheaf of graded algebra? If we have a graded algebra we can construct a projective variety from it. Suppose we are given a graded algebra for every point of the variety and we replaced every point by the corresponding projective space of that graded algebra, that would be a blow up.

A quasicoherent sheaf of graded algebra, is a way of saying that we have assigned a graded algebra to every point of the variety in a nice way.

Example 24.2.1. Simple example of quasicoherent sheaf of graded algebra, suppose our variety is just a point then our quasi... is just a graded algebra, say $k[x_0, \dots, x_n]$ and the blowup is \mathbb{P}^n .

In a rather famous paper, Hironaka showed that we can resolve singularities by repeatedly blowing up. This proof only works in characteristic zero, one of the biggest open problems is to try to generalize it varieties of non-zero characteristic.

Blowing up along ideal

Example 24.2.2. First look at \mathbb{A}^2 with coordinate ring $k[x, y]$. Blowing up at a point corresponds to blowing up along an ideal in $k[x, y]$. So blow up at $(0, 0)$ corresponds to blowup at (x, y) .

Blowing up along a more general ideal is a generalisation of this. Suppose we have an ideal with generators (G_1, \dots, G_n) take:

$$\begin{aligned} & \mathbb{A}^2 \times \mathbb{P}^{n-1} \\ & (x, y, (G_1, \dots, G_n)) \text{ this is defined if } x, y \notin V \end{aligned}$$

We look at the image of $\mathbb{A}^2 \setminus V$ in $\mathbb{A}^2 \times \mathbb{P}^{n-1}$ and take the closure. This is a sort of blowing up corresponding to the ideal.

Example 24.2.3. I is the ideal generated by x^2, y^2 . We map $x, y \in \mathbb{A}^2$ to x, y ($x^2 : y^2$) in $\mathbb{A}^2 \times \mathbb{P}^1$,

If call these variables $x, y, (s : t)$, we have $x^2y^2 = x^2t = y^2s$; we can take $s = 1$:

$$x^2t = y^2$$

This is just the Whitney umbrella all over again, so we introduced singularities by blowing up! We need to be more careful when blowing up, certainly among more complicated ideals. Mysterious but powerful operation.

25 The Atiyah flop

We start by looking at hypersurface $xy = zt$ in $\mathbb{A}^4 = \{(x, y, z, t)\}$. What does this variety look like? It acts like a cone over $\mathbb{P}^1 \times \mathbb{P}^1$. This is because since this is a homogenous equation we can look at this over $(x : y : z : t) \in \mathbb{P}^3$. This is a quadric which we say earlier is a product of two projective lines.

So in affine four space this is more or less a cone over $\mathbb{P}^1 \times \mathbb{P}^1$. This has a singularity at $(0, 0, 0, 0)$ which we resolve by blow up.

$$\begin{array}{ccc} \mathbb{A}^4 & \times \mathbb{P}^2 \\ (x, y, z, t) & (X : Y : Z : T) \end{array}$$

Under the conditions $xy = zt$, $xY = yX$, $xZ = zX$, ... and $XY = ZT$ (since we take Zariski closure)

The point $(0, 0, 0, 0) \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$.

We can check the blowup is non-singular for example, along $X = 1$: $Y = ZT$ with coordinate (x, Y, Z, T) which is a non-singular variety. So we have resolved the singularity.

This exceptional variety can be mapped to \mathbb{P}^1 in two different ways (first or second coordinate), so instead of blowing up the origin to $\mathbb{P}^1 \times \mathbb{P}^1$ we can blow up along \mathbb{P}^1 .

So we take $xy = zt$, and blow up along the line $y = t = 0$:

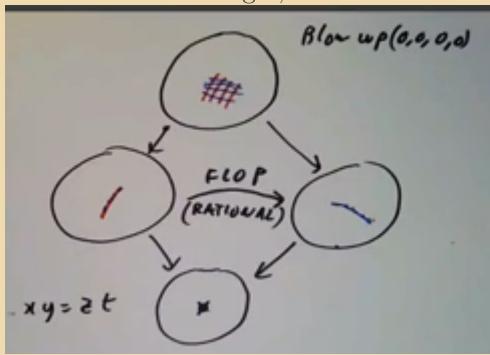
$$\begin{array}{ccc} \mathbb{A}^4 & \times \mathbb{P}^1 \\ (x, y, z, t) & (X : Z) \end{array}$$

With equations $xy = zt$, and $xZ = zX$ and taking the closure we get extra equation $tZ = yX$.

If we take $X = 1$, we get $y = tZ$, $z = xZ$ and $xy = zt$. Which is also non-singular. This time the point $(0, 0, 0, 0)$ is blown up to \mathbb{P}^1 .

(Likewise we can blow up along $x = z = 0$),

Let's draw what we get;



Four varieties are the same except at the coloured points. The Atiyah Flop is the birational map marked on the image. It is a strange map since it takes a copy of \mathbb{P}^1 and changes it to \mathbb{P}^1 embedded in a subtly different way.

The point of this example is to show that there is no minimal way of resolving singularities in general. We would want to have when given a singularity inside a variety, we want a “minimal” resolution of it, a nonsingular variety mapping to it such that any nonsingular variety can be factored through it.

We can't do this here, since there are two ways of resolving the singularity, but not way of resolving it so that they both map through, so no minimal way of resolving. So if we want a minimal model(a resolution of singularites that is as small as possible) we need to allow some mild singularities, the **terminal singularities**.

Lecture 6: Non-singular varieties

26 Singular Points

In this section we will define what a singular point actually is.

Definition 26.1. Let $p = (0, 0, \dots, 0) \in \mathbb{A}^n$, we define a hypersurface $V = \{f = 0\}$, where p is irred polynomial. Then the **Tangent space** at p is the zeroes of linear part of f .

Example 26.1.1. If $f = x - 2y + 3x^2 + 9xy = 0$, then the tangent space is given by

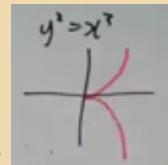
$$x - 2y = 0$$

Definition 26.2. Let $p \in V$, p is called singular if the tangent space at p has greater dimension than dimension of V . (The wrong dimension)

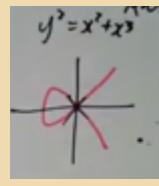
Example with plane curves Let us look at the plane curve given by $f(x, y) = 0$. Then

$$(0, 0) \text{ is singular} \iff f(0, 0) = 0 \text{ and the linear terms vanish}$$

Indeed if the linear terms vanish the tangent is the \mathbb{A}^2 which is of wrong dimension.



Example 26.2.1. $y^2 = x^3$



$y^2 = x^2 + x^3$

n-dimensions This is similar if we have a surface defined by $f(x_1, \dots, x_n)$ then:

$$(0, \dots, 0) \text{ is singular} \iff f(0, \dots, 0) = 0 \text{ and } \frac{\partial f}{\partial x_i}(0, \dots, 0) = 0 \forall i$$

What about codim greater than 1?

Definition 26.3. Let $V \subseteq \mathbb{A}^n$ = zero set of (f_1, f_2, \dots) .

For simplicity we can assume $p = (0, \dots, 0)$ and all the f_i vanish at p . The **Tangent space** is the common zeroes of all linear parts of f_1, f_2, \dots

$$n - \text{rank } \underbrace{\begin{pmatrix} \frac{\partial f_i}{\partial x_j} \end{pmatrix}}_{\text{Jacobian}} = \text{dimension of the tangent space at } p$$

From this we see that the subset of singular points are closed, because a matrix having rank j constant is closed on entries. (Recall we saw this when we say determinantal varieties, this condition is the condition that whole lot of minors of some size vanish).

A tangent space having $>$ than usual is closed condition.

Example 26.3.1. Take the curve given by

$$x^3 + y^3 = 1$$

We find the singular points, we take the derivatives:

$$\begin{aligned} 3x^2 &= 0 \\ 3y^2 &= 0 \end{aligned}$$

This has no singular points over \mathbb{C} , since these equations vanish iff $(x, y) = (0, 0)$ but this point is not on our curve.

HOWEVER over a field of characteristic 3, all points are singular!

What went wrong? Note that over a field of characteristic 3 this is not irreducible, $x^3 + y^3 - 1 = (x + y - 1)^3$.

Theorem 22. For varieties, nonsingular points are dense.

Proof. We just need to show that the set of nonsingular points are nonempty.

(i) Reduce to the case of hypersurfaces. We claim that V is *birational* to a hypersurface.

By showing this we use field theory: let us look at the function field:

$$K = k[\underbrace{x_1, \dots, x_n, \dots}_{\text{alg. indep}}]$$

We can choose x_1, \dots, x_n so that K is separable over $k(x_1, \dots, x_n)$ so generated by one element. So $K = k(x_1, \dots, x_n, y)$ and there is some $f(x_1, \dots, x_n, y) = 0$. Our variety is birational to the hypersurface given by this f .

We can change notation to write our hypersurface as $f(x_1, \dots, x_n) = 0$ and assume that f is irreducible and k is algebraically closed.

All points are singular implies that

$$\frac{\partial f}{\partial x_i} = 0 \text{ at ALL points of } V$$

But $\deg \frac{\partial f}{\partial x_i} < \deg f$, and since f is irreducible $f \mid \frac{\partial f}{\partial x_i}$. But since f divides something of smaller degree we conclude

$$\frac{\partial f}{\partial x_i} = 0 \text{ for all } i$$

This implies $f = 0$ in characteristic zero. In $\text{char } p > 0$ this implies that $f = \sum \text{pth powers of monomials} = \underbrace{g^p}_{\text{in alg closed}}$

But since f is irreducible it can't be the pth power of another polynomial, so $f = 0$.

This contradicts the fact that we have a surface.

Therefore every variety contains a nonsingular point, so the nonsingular points are dense.

□

Remark. At nonsingular points over \mathbb{R} or \mathbb{C} , V looks locally like a smooth manifold (this comes from diff geo). Is the converse true? If V looks locally like a manifold is it nonsingular?

We need to be careful

Example 26.3.2. Over \mathbb{R} , if we take the manifold $y^2 = x^3$, it is a topological manifold but has a singularity.

There is a problem with our definition, they seem to depend about how our varieties are embed into affine space. It is not at all obvious that the tangent space at a point is the same if we embed the same variety into affine space in a different way.

26.1 Zariski tangent space

Definition 26.4. The **cotangent space** at a point p , is $\mathfrak{m}/\mathfrak{m}^2$, where \mathfrak{m} is the max ideal of local ring at p ; recall the local ring at p is ring of functions f/g , such that $g \neq 0$ at p .

The maximal ideal, m can be thought as the functions vanishing at p .

Definition 26.5. The **tangent space** at p , is the dual of the cotangent space at p .

The definition of cotangent space only depends on the local ring and not the embedding of V into affine space. So this definition of the tangent space doesn't depend on the embedding.

Is it equivalent to the earlier definition? If we take $p = (0, \dots, 0)$, and $V \in \mathbb{A}^n$ with coordinates (x_1, \dots, x_n) . The maximal ideal of the local ring at p is generated by x_1, \dots, x_n .

So V is the set of zeroes of (f_1, f_2, \dots) .

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &= (x_1, \dots, x_n)/(f_1, \dots, f_n) \text{ and all monomials of degree } \geq 2 \\ &= \text{vector space spanned by } (x_1, \dots, x_n)/\text{linear parts of } (f_1, \dots, f_n) \end{aligned}$$

This is just the dual of the tangent space defined earlier.

Definition 26.6. The space $\mathfrak{m}/\mathfrak{m}^2$ is called the **Zariski tangent space** for any local ring.

Another way of looking at cotangent space Take a local ring R and look at $\mathfrak{m}/\mathfrak{m}^2$ which is a vector space over the field R/\mathfrak{m} .

The dual $\mathfrak{m}/\mathfrak{m}^2 =$ ring homomorphisms $R \rightarrow k[\epsilon]/(\epsilon^2)$, where $k[\epsilon]/(\epsilon^2)$ is a 2 dimensional vector space with basis elements 1 and ϵ such that $\epsilon^2 = 0$.

This ring homomorphism takes:

$$\mathfrak{m}^2 \rightarrow 0 \text{ and } \mathfrak{m} \rightarrow \text{multiple of } \epsilon$$

What does the above ring look like? Note that $k[\epsilon]/(\epsilon^2)$, is not an algebraic set since the ideal contains nilpotents. This actually corresponds to a scheme, $\text{Spec}k[\epsilon]/\epsilon^2$. This looks like a point with a tangent vector attached to it, and maps from the spectrum of this to the variety correspond to picking a point in the variety and a tangent vector at that point.

Vector fields of smooth manifold V over the reals Let us look at the ring:

$$C(V) = \text{smooth functions}$$

So the space of vector fields is a module over $C(V)$.

We can define:

$$W = \text{cotangent of vec. fields} = \text{dual of the module of vector field}$$

Recall from diff geo that there is a map $d: C(V) \rightarrow W$, which takes f to the 1-form df ; such that d satisfies the Liebnitz rule:

$$d(fg) = f dg + (df)g$$

More generally in algebraic geometry instead of $C(V)$ we might look at the ring; $R = k[x_1, \dots, x_n]/I$.

So we want to find a map

$$d: R \rightarrow W$$

Where W is a module over R , “the module of cotangent vectors”.

How do we construct W ? W is **generated** (as a module) over R by elements of the form dr with $r \in R$, satisfying the relations:

$$dr = 0 \text{ for } r \in kd(fg) = (df)g + f(dg)$$

Then we define W to be the module with these generators and relations.

Example 26.6.1. If $R = k[x_1, \dots, x_n]$. Then W is the free module on elements dx_1, \dots, dx_n . We can also define the module of *tangent vector fields*: $\text{Hom}_R(W, R)$.

In general the module of cotangent vector fields is a bit complicated. It is not usually a free module over the ring, so it is useful to have an alternative description of the module of cotangent space, we define W like this:

Definition 26.7. Suppose we take the homomorphism:

$$R \otimes R \xrightarrow{a \otimes b} R$$

We define I to be the kernel of this map, so it is an ideal of $R \otimes R$, and we can take $W = I/I^2$. W is an R -module: R acts by multiplication on the left R in $R \otimes R$.

We define

$$d: R \rightarrow W \text{ such that } dr = 1 \otimes r - r \otimes 1$$

Problem: Show that this follows the Liebnitz rule.

Problem: Check the universal property. What we mean by this, we want to show: suppose we have any module M with a map from R to M (satisfying the Liebnitz rule). We want to show there is a unique map from W to M , making this diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{d} & M \\ & \searrow d & \uparrow \\ & & W \end{array}$$

We can do this as follows, we have $I \subseteq R \otimes R \rightarrow R$, we can define a map $f: R \otimes R \rightarrow M$ by $f(a \otimes b) = adb$. This gives a map $I \rightarrow M$, we need to check that this map f is 0 on I^2 . Pick some element $\sum s_I \otimes t_i \in I$ and $\sum u_j \otimes v_j \in I$.

This means that

$$\begin{aligned}\sum s_i t_i &= 0 \\ \sum u_j v_j &= 0\end{aligned}$$

We claim that

$$\begin{aligned}f(\underbrace{(\sum s_i \otimes t_i)(\sum u_j \otimes v_j)}_{\in I^2}) &= \sum s_i u_j d(t_i v_j) \\ &= \sum s_i dt_i \sum u_j v_j + \sum s_i t_i \sum u_j dv_j \\ &= 0\end{aligned}$$

From this we can check that W is the universal module such that there is a map from R to W satisfying Liebnitz's rule.

We say the local ring is **regular** if the dimension of the Zariski tangent space is equal to the dimension of the local ring. We say a variety is nonsingular at a point, if its local ring is regular.

27 Du Val singularites

These are also called, simple surface singularites, Kleinian singularites, rational double points or canonical singularites in dimension 2.

We will introduce them by Klein's method.

Klein's method Take a finite group G acting on \mathbb{C}^2 , and take \mathbb{C}^2/G . For reasonable groups G this gives us a variety with a singular point at the origin.

Recall the coordinates ring of \mathbb{C}^2/G is given by $k[x, y]^G$.

Example 27.0.1. Suppose we have a cyclic group of order n generated by σ such that

$$\sigma x = \zeta x \text{ and } \sigma y = \zeta^{-1} x \text{ where } \zeta^n = 1$$

Then the invariants of this action are given by

$$X = x^n, Y = y^n, Z = xy$$

So the coordinate ring is given by

$$k[X, Y, Z]/(Z^n - XY)$$

We can also write this as $Z^n = \frac{(X+Y)^2}{4} - \frac{(X-Y)^2}{4}$

Definition 27.1. The **Du Val singularities** are as follows:

- Cyclic A_n : given by $x^2 + y^2 + z^{n+1} = 0$
- Dihedral D_n : given by $x^2 + zy^2 + z^{n-1} = 0$
- Tetrahedral E_6 : given by $x^2 + y^3 + z^4 = 0$
- Octahedral E_7 : given by $x^2 + y^2 + yz^3 = 0$
- Icosahedral E_8 : given by $x^2 + y^3 + z^5 = 0$

Note for the last case, it is not given by the Icosahedral group of order 60 acting on \mathbb{C}^2 but by the binary Icosahedral group of order 120.

For all of these we are going to work in characteristic zero, and for all of these the only singular point is $(0, 0, 0)$.

Resolving the Icosahedral singularity with Blow ups So we have $x^2 + y^3 + z^5 = 0$, Let $(x_1 : y_1 : z_1)$ be the coordinates for \mathbb{P}^2 , so we look at the subsequeq of $\mathbb{A}^3 \times \mathbb{P}^2$ satisfying the relationships:

$$\begin{aligned} xy_1 &= yx_1 \\ xz_1 &= zx_1 \\ &\vdots \end{aligned}$$

So \mathbb{P}^2 is covered by three copies of \mathbb{A}^2 :

- $x_1 = 1$, we have $y = y_1x$ and $z = z_1x$; so we have:

$$\begin{aligned} x^2 + y_1^3x^3 + z_1^5x^5 &= 0 \\ 1 + y_1^3x + z_1^5x^3 &= 0 \end{aligned}$$

Which we can check has no singularities.

- $y_1 = 1$, we have

$$\begin{aligned} x_1^2y^2 + y^3 + z_1^5y^5 &= 0 \\ x_1^2 + y + z_1^5y^3 &= 0 \text{ no singularities} \end{aligned}$$

- $z_1 = 1$, we have $x = x_1z$, $y = y_1z$

$$\begin{aligned} x_1^2z^2 + y_1^3z^3 + z^5 &= 0 \\ x_1^2 + y_1^3z + z^3 &= 0 \end{aligned}$$

Taking the partial derivatives:

$$\begin{aligned} 2x_1 &= 0 \\ 3y_1^2z &= 0 \\ 3z^2 &= 0 \end{aligned}$$

So we have a singular point at $x_1 = y_1 = z = 0$

So now we resolve the singularity at $x_1^2 + y_1^3z + z^3 = 0$; again we take $\mathbb{A}^3 \times \mathbb{P}^2$ where \mathbb{P}^2 has coordinates $(x_2 : y_2 : z_2)$. Once again we cover \mathbb{P}^2 with three copies of \mathbb{A}^2 :

- Like before we can check that $x_2 = 1$ and $z_2 = 1$ yield no singularities.
- When $z_2 = 2$: we have $z = z_2y_1$ and $x_2 = x_1y_1$

$$\begin{aligned} x_2^2y_1^2 + y_1^4z_2 + y_1^3z_2^3 &= 0 \\ x_2^2 + y_1^2z_2 + y_1z_2^3 &= 0 \end{aligned}$$

This has a singularity at $(0, 0, 0)$.

We don't seem to have made any progress, but we actually have the new singularity is simpler than the previous one.

Again we blow up this singularity, with new coords $(x_3 : y_3 : z_3)$:

- $x_3 = 1$: No singularities
- $y_3 = 1$: $x_3^2y_1^2 + y_1^3z_3 + y_1^4z_3^3 = 0$

The only singularity is at $x_3 = y_1 = z_3 = 0$.

- $z_3 = 1$: $x_3^2 + y_3^2z_2 + y_3z_2^2 = 0$

so a singularity at $x_3 = y_2 = z_2 = 0$

We now have two singularites to look at:

(1)

$$x_3^2 + y_1 z_3 + y_1^2 z_3^3$$

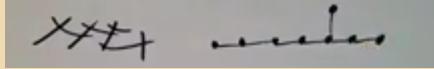
We blow up introducing $(x_4 : y_4 : z_4)$; and at $x_4 = 1, y_4 = 1$ and $z_4 = 1$ we have no singularites.

(2)

$$x_3^2 + y_3^2 z_2 + y_3 z_2^2 = 0$$

We blow up introducing $(x_5 : y_5 : z_5)$. At $x_5 = 1$ we get no singularites, but at $y_5 = 1$ we get 2 singularities and at $z_5 = 1$ we get 2 singularities. But one of the singularites of $y_5 = 1$ is the same as a singularity in $z_5 = 1$; so we have three singularites to resolve.

If we take each of these three singularites and blow them up once we get something non-singular. So after eight blowups we end up with something nonsingular, each blowup introduces a exceptional curve that looks like \mathbb{P}^1 and when they intersect they look like this:



If we draw a point for each lines and connect the points if the corresp lines intersect, we get the E_8 Dynkin diagram as seen above.

We see that a problem with Blow up involves a lot of book keeping and each don't do very much, we only make a tiny improvement to our singularity. Furthermore unlike in this example, if we blow up a point we can find the singularities form a subset of dimension greater than 1.

28 Resolution of singularites

Example 28.0.1. The first of resolution of singularites we are going to look at is the equation:

$$x^4 + y^4 = z^2$$

Remark. This is a historically famous equation since it was used by Fermat to show $x^4 + y^4 = z^4$ has no integer solutions.

We find singularites by differentiating:

- $4x^3 = 0$
- $4y^3 = 0$
- $2z = 0$

So the only singular point is at the origin. So let us resolve it by blowing up at $(0, 0, 0)$ introducing new variables $(X : Y : Z)$.

- $Z = 1$: $x = zX$ and $y = zY$. So

$$\begin{aligned} z^4 X^4 + z^4 Y^4 &= z^2 \\ z^2 X^4 + z^2 Y^4 &= 1 \end{aligned}$$

We can check that this is nonsingular.

- $Y = 1$ $x = yX$ and $z = yZ$. So

$$\begin{aligned} y^4 X^4 + y^4 &= y^2 Z^2 \\ y^2 X^4 + y^2 &= Z^2 \end{aligned}$$

By differentiating with respect X, y, Z we get:

- $y^2 4X^3 = 0$
- $2y(X^4 + 1) = 0$
- $2Z = 0$

So we get singular points when $y = Z = 0$.

- $X = 1$: Similarly to $Y = 1$, we get a line of singular points.

This is different from the du Val singularities from last time, we get a whole line except of points. We might think this made things worst since the dimension of singularity got bigger, but that is not true. The nastiness comes from the codimension, so turning a point to a line is actually good.

So let us finish resolving it, we get the equation

$$y^2X^4 + y^2 = Z^2$$

And we blow up along the line $y = Z = 0$. Let us introduce two new variables from a copy of \mathbb{P}^1 , $(s: t)$, such that $sZ = tY$. Covering the projective line by two copies of affine line:

- $s = 1$: We find $z = ty$, and our equation becomes:

$$\begin{aligned} y^2X^4 + y^2 &= t^2y^2 \\ x^4 + 1 &= t^2 \end{aligned}$$

Which is nonsingular.

- $t = 1$: We again find we get a nonsingular line.

When things go wrong This example illustrates that if we choose our blow up badly we can make the singularity worst.

Example 28.0.2. Let us look at $x^2 - yz = 0$, this is a cone with a singularity at the origin. Suppose instead of blowing up at the origin as we did before, we blow up at the line $y = z = 0$.

So we introduce two new coordinates $(Y: Z) \in \mathbb{P}^1$, with $yZ = zY$.

- $Y = 1$: $z = yZ$ our equation becomes $x^2 - y^2Z = 0$ the Whitney umbrella. We started with a simple singularity and we have a more complicated singularity.
- $Z = 1$

We need to be careful of where we blow things up, it can make things worst.

Example from number theory

Example 28.0.3. We can look at $\mathbb{Z}[\sqrt{-3}]$, this ring has a problem since it doesn't have unique factorization:

$$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

We pretend that $\mathbb{Z}[\sqrt{-3}]$ is a coordinate ring of a variety (in actuality it is the coordinate ring of a scheme). What are the points of this variety? They correspond to maximal ideals for example

$$(2, \sqrt{-3} - 1)$$

We shall show that in some sense, the variety (scheme) has a singular point at this point.

The local near this point is $R = \mathbb{Z}_{(2)}[\sqrt{-3}]$, where $\mathbb{Z}_{(2)}$ is the ring we get by inverting all primes not equal to 2; i.e. $\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = 1 \text{ and } b \equiv 1 \pmod{2} \right\}$.

The maximal ideal of this local ring:

$$(2, \sqrt{-3} - 1) = \mathfrak{m}$$

We have:

$$R/\mathfrak{m} = \mathbb{F}_2$$

Indeed take the map $\varphi\left(\frac{a}{b} + \frac{c}{d}\sqrt{-3}\right) = a + c$. Since $\varphi\left(\frac{a}{b} + \frac{x}{y}\right) = \varphi\left(\frac{ay+bx}{xy}\right) = ay + bx = a + x$, since $y = b \equiv 1 \pmod{2}$. And $\varphi\left(\frac{a}{b}\frac{x}{y}\right) = ax$, we see that this map is a homomorphism with kernel \mathfrak{m} ,

Likewise we can easily check that R/\mathfrak{m}^2 has order 8. So

the cotangent space at the point corresponding to the max ideal $\mathfrak{m}/\mathfrak{m}^2$ has order 4

And is a two dimensional vector space over R/\mathfrak{m} . We find that the Krull dimension of R has dimension 1. So the cotangent space at \mathfrak{m} has larger dimension than R , so this corresponds to a singular point (in some sense as it is not exactly a variety).

The fact that $\mathbb{Z}[\sqrt{-3}]$ has a singular point actually implies that it is not a UFD.

Resolving the singularity We can solve this by blowing up, but we won't do it. In number theory we resolve singularities by taking a normalization or integral closure of a ring. Taking the integral closure of

$$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\underbrace{\frac{\sqrt{-3} + 1}{2}}_{\omega}]$$

So $\omega^2 + \omega + 1 = 0$, so ω is an algebraic integer in the field of our first ring.

The new ring does have unique factorization and its points are nonsingular. Taking the integral closure of our ring is sort of the same as taking the desingularisation of our variety.

Application of resolution of singularities Recall the Gamma function:

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}, \text{ with } \operatorname{Re}(s) > 0$$

We can extend this to a meromorphic function of s by integrating by parts.

Now suppose we have:

$$\int |f(x_1, \dots, x_n)|^s \varphi(x_1, \dots, x_n) dx_1 \dots dx_n$$

Where f is a polynomial and φ is smooth with compact support. Note that $|f(x_1, \dots, x_n)|^s$ is a holomorphic function of s , if the real part of s is large.

Can we analytically continue to all s ? We see that this is more or less the same as the Gamma function, f corresponds to t and φ corresponds to e^{-t} . (Realise that e^{-t} , doesn't have compact support but Borcherds doesn't really care about that).

Problem: Occurs at the zeroes of f . The zeroes of f is some sort of hypersurface with singularities. The more complicated the singularities are the more difficult it is to figure out what is going with this integral.

By Atiyah, there is a very easy way to settle this question. We only need to resolve singularities of the variety $f = 0$. What we end up with is not actually a nonsingular space, since when we blow up singularities according to Hironaka we introduce exceptional curves. The exceptional curves don't really matter because they all cross transversally. So we end up with things that look like $x_1 x_2 \dots x_k = 0$, a lot of hyperplanes intersecting with each other.

We are reduced to the case

$$\int |x_1 \dots x_k|^s \varphi(x_1, \dots, x_n) dx_1 \dots dx_n = 0$$

This splits as a lot of integrals of the form $\int |x_1|^s f(x_1) dx_1 = 0$, and we can do this in the same as the gamma function by integrating by parts.

So resolving singularities allow us to prove the existence of meromorphic continuations of integrals as above.

Bernstein found another to prove this, with polynomials he introduced, which are called *Bernstein-Sato polynomials*.

29 Completions of a ring

Example 29.0.1. Suppose we take the ring of polynomials

$$k[x] = \sum_{i=0}^n a_i x^i$$

The completion is the ring of formal power series

$$k[[x]] = \sum_{i=0}^{\infty} a_i x^i$$

How do we construct the formal power series ring from the polynomial ring?

If we let $k[x] = R$, we take the ideal $I = (x)$ and we have:

- $R/I = k = \{a_0\}$
- $R/I^2 = \{a_0 + a_1 x\}$

- $R/I^3 = \{a_0 + a_1x + a_2x^2\}$
- \vdots

An element of the completion, means we pick elements of one of these rings, and they have to be compatible, so if we pick an element in R/I^2 is must have an image in R/I .

So we have a sequence of rings:

$$\begin{array}{ccccc} & \xleftarrow{\quad} & R/I^3 & \xrightarrow{\quad} & R/I^2 & \xrightarrow{\quad} R/I \\ & \searrow & \nearrow & \uparrow & \nearrow & \\ & & \hat{R} & & & \end{array}$$

And we pick an element in each of these rings that are all compatible, i.e. commute with these automorphisms; that is an element of the power series ring, which we call the completion \hat{R} .

This works for any ring R and any ideal I .

Example from number theory

Example 29.0.2. If we take $R = \mathbb{Z}$ and $I = (p)$ for a prime p ; then $\hat{R} = \mathbb{Z}_p$, the p -adic integers.

Definition 29.1. What we usually do in algebraic geometry, we take R = a local ring, and \mathfrak{m} = max ideal. And we look at the completion with respect to this local ring:

$$\hat{R} \text{ given by } R/\mathfrak{m}^3 \rightarrow R/\mathfrak{m}^2 \rightarrow R/\mathfrak{m}$$

Is the map

$$R \rightarrow \hat{R}$$

injective? Yes if R is Noetherian, but no in general.

Example 29.1.1. Let R = smooth functions on \mathbb{R} and $I = (x)$ = functions vanishing at zero.

Then R/I^n are power series where we ignore all terms greater than n , so \hat{R} is just power series.

However the map

$$R \rightarrow \hat{R}$$

Is not injectivem since for example we can have smooth function that vanish to all orders at 0, for example the function

$$f(x) = \begin{cases} e^{1/x^2} & \text{for } x \neq 0 \\ 0 & \text{for } x = 0 \end{cases}$$

This function is in the kernel of the map from R to its completion.

More algebraic example

Example 29.1.2. Take

$$R = k[[x, x^{1/2}, x^{1/4}, \dots]]$$

By this we mean take the union of the power series:

$$k[[x]] \rightarrow k[[x^{1/2}]] \rightarrow k[[x^{1/4}]]$$

Take the ideal:

$$I = (x, x^{1/2}, x^{1/4}, \dots)$$

Note that $I = I^2$, so

$$\hat{R} = k$$

The map from R to the completion in this case fails badly to be injective.

29.1 Hensel's lemma

This lemma is not just one lemma but many, since there are a lot of variations of this lemma.

Lemma 23. *Solutions in R/\mathfrak{m} can be lifted to solutions in \hat{R} under some conditions.*

Typical example Suppose $f(z) = g_0(z)h_0(z) \pmod{m}$, where $g_0, h_0 \in k[z]$ and $f \in R[z]$. Then this lifts to

$$f(z) = g(z)h(z) \text{ where } g, h \in R[z]$$

If g_0, h_0 are coprime in $k[z]$.

Sketch of idea of proof

Proof. Suppose $f = gh \pmod{m^n}$, try to find a, b such that:

$$f = (g + a)(h + b) \pmod{m^{n+1}}$$

Here $a, b \in \mathfrak{m}^{n+1}/\mathfrak{m}^{n+2}$.

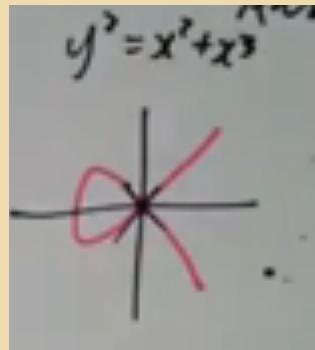
If we do this we need to solve:

$$g_0b + h_0a = (\text{complicated})$$

The idea is that we can solve this equation, since g_0 and h_0 are coprime. Since two coprime elements generate the unit ideal. \square

The advantage of complete local ring over local rings, is that it is very easy to solve equations and find roots of equations since we have multiple versions of Hensel's lemma.

Example 29.1.3. Let $y^2 = x^3 + x^2$, which looks like:



Note if we look really close the origin, it sort of looks like two lines crossing:

×

Which is the graph of $x^2 = y^2$.

We can't really see this with the local ring, since if it was the union of two components it would have zero divisors, but it is the subring of a field. The local ring isn't aware that near the origin, it splits into two components.

Let R = local ring at $(0, 0)$ = i.e. the coordinate ring of R and inverting everything that doesn't vanish at $(0, 0)$

The completion of the local ring is:

$$\hat{R} = k[[x, y]]/(y^2 - x^3 - x^2)$$

The point is that $y^2 - x^2 - x^3 = (y - x)(y + x) \pmod{I^2}$, so by taking Hensel's lemma or square roots directly we see that:

$$y^2 - x^2 - x^3 = (y - x + \text{power series})(y + x + \text{power series})$$

So over the completion of the local ring we do see that there are two components, each factor corresponds to a component of the \times graph.

Furthermore, whilst the local ring R has no zero divisors, but the completion has zero divisors. So completions may cause problems, c.f. Henselazation

Definition 29.2. Analytically isomorphic means that the completions of the local ring are isomorphic with each other.

Series of rings

$$R \rightarrow \hat{R} \rightarrow \dots \rightarrow R/\mathfrak{m}^3 \rightarrow R/\mathfrak{m}^2 \rightarrow R/\mathfrak{m} = k$$

We can think of these rings as corresponding to finer and finer nbhs of a point.

- R/\mathfrak{m} , is the coordinate ring of a point
- R/\mathfrak{m}^2 , is the coordinate ring of a point, with a “tiny bit sticking out”, the first order neighbourhood of a point.
- R/\mathfrak{m}^3 , looks like a point with “two more points in the same place”
- ...
- \hat{R} , looks like a point with a short smooth curve sticking out of It
- R , the local ring looks like the line with a finite number of points missing.

30 Elimination theory

Remark. c.f. Theorem 5.7 from Hartshorne.

Elimination theory has caused a fair amount of controversy, André Weil in his book “Foundations of algebraic geometry” had a rather scathing critique of it. It was also talked about in Abhyankar’s poem “Polynomials and Power series, may they forever rule the world!”

But what is elimination theory?

Example 30.0.1. Suppose we have two polynomials

$$x^3y^4 - 7x^2 - xy^8$$

and

$$3x^2y^5 + 4y^2 + x^4y^7$$

We eliminate y , by this we mean we find an expression for y with the first polynomial, and we substitute it in the second polynomial.

This is hard, since by Bézout’s theorem there should be $9 \cdot 11 = 99$ points of intersection, so x should satisfy a polynomial of degree 99. How do we write out this polynomial?

General problem Suppose we have:

$$\begin{aligned} f(x) &= \sum_{i=0}^m a_i x^i \\ g(x) &= \sum_{i=0}^n b_i x^i \end{aligned}$$

What is the condition for a common root? For now we assume $a_m \neq 0$ and $b_n \neq 0$. If these have a common root then:

$$f(x)p(x) = g(x)q(x)$$

For some $p, q \neq 0$ with $\deg p < n$ and $\deg q < m$. Indeed if they have a common root just put

$$p = \frac{g}{x - \alpha}, \text{ and } q = \frac{f}{x - \alpha}$$

Where α is the common root.

So the condition for a common root is to find such p, q such that $fp = gq$. If we expand it out we get a whole bunch of homogenous linear equations whose coeffs depends on the a_i, b_j . If this set of homogenous equations has a non-trivial solution then, some big determinant vanishes.

$$\left| \begin{array}{cccccc} a_m & a_{m-1} & \dots & a_0 & 0 & 0 & 0 \\ 0 & a_m & \dots & a_1 & a_0 & 0 & 0 \\ \vdots & & & & & & 0 \\ 0 & 0 & \dots & a_m & \dots & a_1 & a_0 \\ b_n & \dots & & & b_0 & \dots & 0 \\ 0 & b_n & \dots & & b_1 & b_0 & 0 \\ \vdots & & & & & & b_0 \\ 0 & 0 & \dots & b_n & \dots & & b_0 \end{array} \right| = 0$$

SYLVESTER MATRIX RESULTANT

The matrix looks like:

Definition 30.1. This determinant is called the **resultant**.

Problem: What to do when $a_m = b_n = 0$? The condition that $a_m = 0$ can be thought as the polynomial having a root at infinity. If we take the corresp homogenous poly:

$$a_m x^m y^0 + \dots + a_0 x^0 y^m$$

Then we can think of a root being a point in $(x: y) \in \mathbb{P}^1 = k \cup \infty$, where k is equiv $(x: 1)$ and ∞ corresponds to $(1: 0)$.

So the resultant is zero, is equivalent to the two homogenous polynomials:

$$f(x) = \sum_{i=0}^m a_i x^i y^{m-i} g(x) = \sum_{i=0}^n b_i x^i y^{n-i}$$

have a common zero in $\mathbb{P}^1 = k \cup \infty$.

Example When does the polynomial $f(x) = ax^2 + bx + c$ have a double root. Well note it has a double root if f and $f'(x) = 2ax + b$ have a common zero.

The resultant:

$$\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = ab^2 - b(2ab) + c(4a) = -a \underbrace{(b^2 - 4ac)}_{\text{discriminant}}$$

So if a is non-zero, then f has a double root if and only if the discriminant is zero. (If $a = 0$, recall f and f' have a root at infinity).

More complicated example Suppose $f(x) = x^3 + bx + c$, when does this have a double root? Well $f'(x) = 3x^2 + b$, we look at the Sylvester matrix:

$$\begin{vmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{vmatrix} = 4b^3 + 27c^2$$

This is not quite the discriminant of a cubic, there is a sign problem the discriminant is $-4b^3 - 27c^2$. In all cases the polynomial has a double root if this discriminant is zero.

Lecture 7: Nonsingular curves

31 Informal review of classification of algebraic curves

We are going to look at algebraic curves over \mathbb{C} to simplify this. There are three ways of viewing algebraic curves over \mathbb{C} :

- Algebraic curves, this is birational to a complete curve since we can embed it in projective space and take its closure. Furthermore, we will see later that it is birational to a **nonsingular** projective curve.
- nonsingular projective curves are more or less the same as a compact Riemann surface.
- nonsingular projective curves also correspond to f.g. fields over \mathbb{C} of transcendence degree equal to 1.

So there are three ways of looking at the same object. An analyst talks about compact Riemann surface, a algebraist talks about f.g. fields over \mathbb{C} of transcendence degree equal to 1 and a geometer talks about nonsingular projective curves.

Genus

Definition 31.1. The **genus** is the basic invariant of a curve.

It is easy to talk about the genus of compact Riemann surface (look at the holes), defining the genus for algebraic curves can be done but involves a bit more work.

For each genus there is a family of curves of that genus, and something called a **moduli space** whose points correspond to isomorphism classes of curves of that genus.

It is a fundamental problem to try to understand this moduli space, which is more or less equivalent to classifying all curves of a given genus.

- Genus 0: Is easy, the only nonsing curve of genus 0 is \mathbb{P}^1 ,
- Genus 1: Elliptic curves, as we saw these are of the form \mathbb{C}/L where $L =$ is a lattice $m + n\tau$.

When are two elliptic curves the same? If we have any three points on the projective line there is a linear fractional transformation:

$$\tau \rightarrow \frac{a\tau + b}{c\tau + d}$$

Taking any points $\lambda_1, \lambda_2, \lambda_3$ to $0, 1, \infty$ respectively and λ_4 to some point λ .

So any elliptic curve over \mathbb{C} can be defined by giving a point λ and we are looking at the equation:

$$y^2 = x(x - 1)(x - \lambda)$$

However two values of λ can sometimes give the same algebraic curve. For example, there is a group of order 6 permuting, $0, 1, \infty$ which takes

$$\lambda \rightarrow \begin{cases} \lambda \\ 1 - \lambda \\ \frac{1}{\lambda} \\ \frac{1}{1-\lambda} \\ \frac{\lambda}{\lambda-1} \\ 1 - \frac{1}{\lambda} \end{cases}$$

This gives a group of order 6 isomorphic to S_3 , and this acts on λ . Any two λ that are equivalent on this group of order 6 give the same elliptic curve since they just permute the λ_i .

So it turns out that

$$\text{Moduli space} = \text{affine line param by } \lambda/S_3$$

In order to take the quotient of the affine line by this group of order 6, we want to find the invariants of this action.

Definition 31.2. j-invariant

$$j = \frac{256(\lambda^2 - \lambda + 1)}{\lambda^2(\lambda - 1)^2}$$

Is an invariant of this action.

Recall that we also said that elliptic curves can be given by $\mathbb{C}/\langle 1, \tau \rangle$; so given τ there is a corresponding j -invariant:

Definition 31.3. If $q = e^{2\pi i\tau}$, then

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

So two elliptic curves are isomorphic, iff they have the same j -invariant. So the moduli space is more or less isomorphic to the affine line \mathbb{A}^1 (not really since the moduli space of elliptic curve is not really a variety it is something called an **Algebraic stack**).

Genus 2 curves We can write down genus 2 curves in a similar way to how we write genus 1 curves.

$$y^2 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)(x - a_5)(x - a_6)$$

So we are taking six points in \mathbb{C} and taking a curve that is ramified to order two at these six points.

In general If we have a curve of the form

$$y^2 = (x - a_1) \cdots (x - a_{2n})$$

We can work out the Euler characteristic as: $\chi = 2 + 2n - 4n + 2 = 402n = 2 - 2g$, so $g = n - 1$.

Remark. This also shows that there are curves of any genus.

Definition 31.4. Curves of the above form are called **hyperelliptic curves**.

It turns out in genus 2 all curves are hyperelliptic, so this gives all of them.

Classifying curves of genus 2 The classification is equivalent to taking distinct six points in \mathbb{P}^1 and modding by the action of the group $PSL_2(\mathbb{C})$,

Taking six distinct points of the projective line is more or less the same as classifying binary forms of degree six:

$$a_0x^6 + a_1x^5y + \cdots + a_6y^6 / SL_2(\mathbb{C})$$

This is the problem of classifying invariants of binary quantics.

This looks like $\mathbb{A}^3/(Z/5Z)$, where $(x, y, z) \rightarrow (\zeta x, \zeta^2 y, \zeta^3 z)$, where $\zeta^5 = 1$. The set of generators of this are:

$$\langle x^5, x^3y, xy^2, y^5, x^2z, xz^3, z^5, yz \rangle$$

There is no similar description of moduli space in higher dimension, it gets too complicated.

Genus 3 Genus 3 curves include:

- hyperelliptic; $y^2 = (x_1 - a_1) \cdots$
- degree 4 nonsingular curves in plane

Remark. Genus of degree d nonsingular plane curve:

$$\chi = 2d - d(d-1) = 2 - 2g \Rightarrow g = \frac{(d-1)(d-2)}{2}$$

So:

g	d
0	2
1	3
3	4
6	5

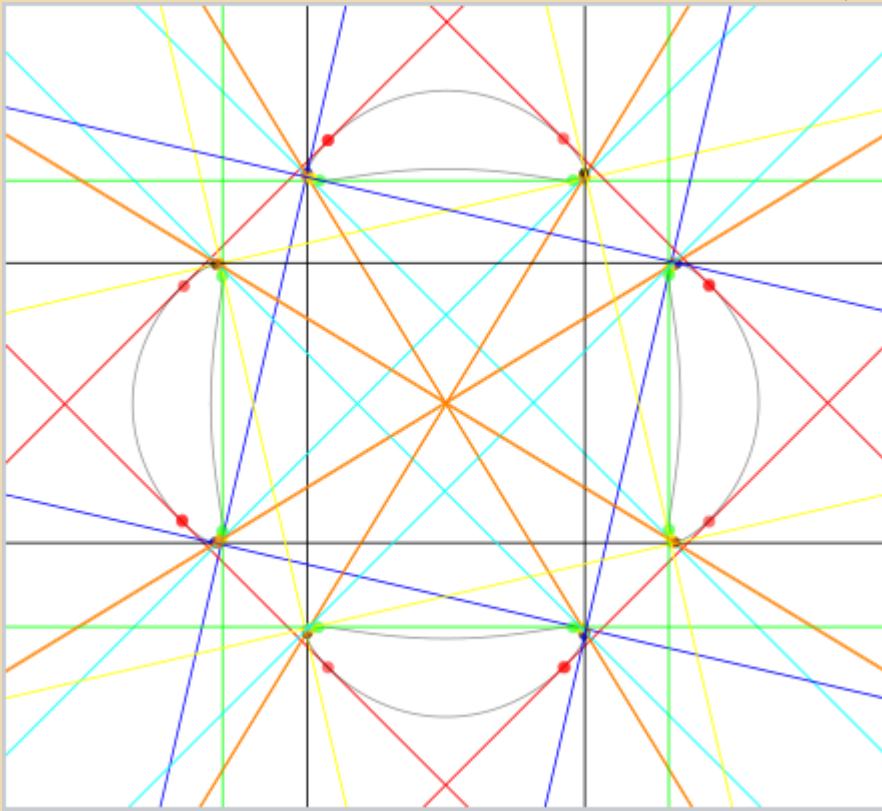
So it is quite unusual for an algebraic curve to be nonsingular plane curve.

There is in fact a six dimension family of degree four nonsingular curves in the plane. On the other hand the hyperelliptic curves form a family of dimension 5.

Trott curve: example of genus 3

$$44(x^4 + y^4) - 255(x^2 + y^2) + 350x^2y^2 + 81 = 0$$

This is an example of a curve where we can see all of its 28 bitangents (lines meeting the curve twice).



Genus 4 and 5

- Genus 4, given by the intersection of cubic and quadric in \mathbb{P}^3
- Genus 4, given by the intersection of three quadric in \mathbb{P}^4

The higher the genus, the more complicated it is to describe what the curves look like. Representing curves of high genus is difficult.

32 Hurwitz curves

They are the most symmetric curves of genus g .

- $g = 0$: The only curve is projective line, and group of automorphisms is infinite
- $g = 1$: This is an elliptic curve, again the group of automorphisms is infinite
- $g > 1$: Here Hurwitz proved that the order of the automorphism group $|G| \leq 84(g - 1)$. If characteristic is zero.

Idea of the proof We look at the **Orbifold Euler char**. Recall if we have a surface, then the euler characteristic is:

$$\chi = n_2 - n_1 + n_0 \text{ where } n_i = \text{ number of cells of dim } i$$

In general the Euler characteristic for a compact orientable surface is

$$\chi = 2 - 2g$$

Definition 32.1. Orbifolds are given by

surface/finite group

(at least for our purposes in general they can be more complicated)

The idea is that we have a point fixed by the subgroup H . Then when working with the Euler characteristic the quotient of the point by the group H should be thought as only $\frac{1}{|H|}$ of a point.

Example 32.1.1. Suppose we have a disc and we take an automorphism of order two that rotates by 180 degrees. If we quotient out by this we have a sort of cone and the vertex of the cone counts only as half a point.

Remark. Key point If we have a surface S then:

$$\chi(S/|G|) = \frac{\chi(S)}{|S|}$$

Furthermore we can consider the orbifold $S/|G|$ as a surface, and consider the regular Euler characteristic on it. So we find this definition:

Definition 32.2. Suppose the orbifold

$$S/G = \text{surface } T \text{ with conical singular points of order } p_1, p_2, \dots$$

Then the

$$\text{Orbifold } \chi = \text{Topological } \chi - (1 - \frac{1}{p_1}) - (1 - \frac{1}{p_2}) - \dots$$

We want to show: That the maximal value of this is $-\frac{1}{42}$. Where does this come from? The topological euler charn will be $2 - 2h$, for some h where h is the genus of the topological surface. And each of the $(1 - \frac{1}{p})$ can be equal to $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots$ Since $g > 1$ we have $\chi < 0$ so this is a negative number and we want to make it as close to zero as possible.

1. $h = 0$, since if $h > 0$, then

$$2 - 2h - (1 - \frac{1}{p_1}) \dots$$

This is either zero which is not allowed or $\leq \frac{-1}{2} \leq \frac{-1}{42}$

2. Suppose there are ≤ 2 conical points, then the char is $2 - (1 - \frac{1}{p_1}) - (1 - \frac{1}{p_2}) > 0$, which is not allowed.

3. Suppose there are ≥ 4 conical points, then $2 - (1 - \frac{1}{p_1}) - \dots - (1 - \frac{1}{p_1}) \leq \underbrace{\frac{-1}{6}}_{2,2,2,3} \leq \frac{-1}{42}$

4. So there are exactly three conical points, p_1, p_2, p_3 .

Examining p_1, p_2, p_3 Suppose there are no conical points of order 2, then:

1. $3, 3, 3$ which gives us $2 - \frac{2}{3} - \frac{2}{3} - \frac{2}{3} = 0$
2. $3, 3, 4$ which gives us $2 - \frac{2}{3} - \frac{2}{3} - \frac{3}{4} = \frac{-1}{12} < \frac{-1}{42}$
3. Anything else gives us a number even smaller than $\frac{-1}{12}$.

So we can't have zero conical points of order two. So there is at least one point of order 2.

Examining $2, p_2, p_3$ If there are two points of order two:

$$2 - 0.5 - 0.5 - (1 - \frac{1}{p_3}) > 0$$

Which is impossible.

So there is exactly one point of order 2.

The case where $p_2, p_3 \geq 4$

1. $2, 4, 4$; $2 - \frac{1}{2} - \frac{3}{4} - \frac{3}{4} = 0$.
2. $2, 4, 5$; $2 - \frac{1}{2} - \frac{3}{4} - \frac{4}{5} = \frac{-1}{20} < \frac{-1}{42}$.
3. Anything else will be smaller than $\frac{-1}{20}$.

So we can't have both points of order ≥ 4 :

Examining $2, 3, p_3$ So now suppose $p_3 > 2$:

- $p_3 = 3$: Euler char: $\frac{1}{6}$, not allowed since Euler char must be < 0
- $p_3 = 4$: Euler char: $\frac{1}{12}$, not allowed since Euler char must be < 0
- $p_3 = 5$: Euler char: $\frac{1}{30}$, not allowed since Euler char must be < 0
- $p_3 = 6$: Euler char: 0, not allowed since Euler char must be < 0
- $p_3 = 7$: Euler char: $\frac{-1}{42}$
- $p_3 = 8$: Euler char: $\frac{-1}{24} \leq \frac{-1}{42}$
- $p_3 > 8$: Euler char: $< \frac{-1}{24} \leq \frac{-1}{42}$

If $\chi < 0$, then $\leq \frac{-1}{42}$ so:

$$\frac{2 - 2g}{|G|} \leq \frac{-1}{42} \text{ if } < 0$$

$$\therefore |G| \leq 84(g - 1)$$

Moreover if this bound is satisfied this implies G is generated by α, β, γ where $\alpha^2 = 1$, $\beta^3 = 1$, $\gamma^7 = 1$ and $\alpha\beta\gamma = 1$. Such a finite group is called a **Hurwitz group**.

32.1 Example of Hurwitz curves

For genus $g \leq 1$ we still get interesting information on G .

- If $g = 0$: This is the case when the orbifold euler char is positive, there aren't that many those give us the orders of a finite group of automorphisms of a genus 0 surface (more or less a sphere). The smallest positive value is:

$$\frac{2}{|G|} = 2 - \frac{1}{2} - \frac{2}{3} - \frac{4}{5} = \frac{1}{30}$$

So a finite value of $|G| < \infty$ acting on \mathbb{P}^1 is 60.

- If $g = 1$: The orbifold characteristic is zero, so the choices for p_i can be

$$\{p_i\} = \begin{cases} \{\} \\ \{2, 2, 2, 2\} \\ \{3, 3, 3\} \\ \{2, 4, 4\} \\ \{2, 3, 6\} \end{cases}$$

These correspond to various finite cyclic groups acting on elliptic curve and fixing a point.

Genus $g = 2$: Most symmetric curve? Can we find a genus 2 curve with automorphism group G of order 84? The answer is **no**.

Suppose $|G| = 84$, by the Sylow theorems, G has a normal subgroup of order 7 (since $84 = 2^2 \cdot 3 \cdot 7$). So the quotient of G and this group of order seven, has order 12 and has a normal subgroup of order 3 or 4 by the Sylow theorems. In the second case, if it is of order 4, then any element of order 2 or 7 is in the normal subgroup of order 28 which has no elements of order 3. So there are no elements of order 2 and 7 whose product is of order 3. This is a contradiction since any Hurwitz group has three elements a, b, c such that $a^2 = b^3 = c^7 = abc = 1$.

The case where $G/7$ has a normal subgroup of order 3 causes a similar contradiction.

So in all cases a group of order 84 can't be generated by three elements as above, so it can't be a Hurwitz group.

But recall that if $|G| \neq 84(g - 1)$, then $|G| \leq 48(g - 1)$.

Example 32.2.1. We can take the **double branched cover of \mathbb{P}^1** , branched over $0, \infty, 1, -1, i, -i$. We can think of this as being something like the vertices of an octohedron. So the point is the subgroup of $PSL_2(\mathbb{C})$ fixing this set of six points is generated by the following automorphism:

$$z \rightarrow iz$$

$$z \rightarrow \frac{z+1}{1-z}$$

What about $g = 3$? In this case there is a Hurwitz curve given by the **Klein quartic**:

$$x^3y + y^3z + z^3x = 0 \subseteq \mathbb{P}^2$$

We can check that this is nonsingular and the genus of a degree four nonsingular curve is 3. And up to isomorphism this is the only genus 3 curve whose automorphism group achieves the bound $84(g - 1) = 168$.

Its automorphism group is in fact:

$$PSL_2(F_7)$$

Which is a simple group of order 168, the next smallest simple group after A_5 of order 60.

Remark. This upper bound fails in characteristic $p > 0$. This proof doesn't work since we can't define the Euler characteristic in a way that behaves as in characteristic zero.

33 Desingularising an algebraic curve

Recall f.g. function fields of transcendence degree 1 corresponds to nonsingular proj curves. (c.f. Hartshorne)

First of all if a function field has transcendence degree 1 and is f.g., then it is generated by two elements it is of the form $k(x, y)$ with x transcendental over k . And there is some polynomial $f(x, y) = 0$. This gives us a projective curve possibly singular.

How do we get rid of the singularities? How do we resolve singularities of curves?

Newton We can resolve singularities of $f(x, y) = 0$ by repeated blow ups. We will assume that $\text{char} = 0$. This proof doesn't work in $\text{char } p$ but the result is still true.

Proof. We assume the singular point is $(0, 0) \subseteq \mathbb{A}^2$, we look at the lowest degree terms:

$$a_n y^n + a_{n-1} y^{n-1} x + \cdots + a_0 x^n + (\text{degree } > n)$$

n is called the multiplicity of the singularity.

The lowest degree terms form a homogenous polynomial so they have roots in \mathbb{P}^1 . These roots correspond to the directions of the singularity.

Blowing up the point means separating out the different directions. One blow up reduces the multiplicities *unless* all n points of \mathbb{P}^1 are the same.

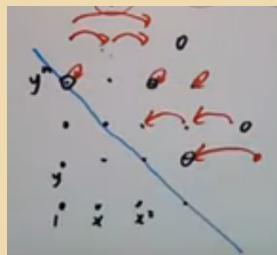
$$\text{i.e. } a_n y^n + \cdots + a_0 x^n = a_n(y + \alpha x)^n \text{ for } a_n \neq 0$$

So we can concentrate on the case where all the n roots are the same. By a change of variable: $y \rightarrow y - \alpha x$, then we get $y^n + (\text{terms of degree } > n)$.

Example 33.0.1. Suppose we have $y^2 + x^9 + y^5 x^3$, if we blow it up we change $y \rightarrow yx$ and we get:

$$y^2 x^2 + x^9 + y^5 x^5 x^3 = 0 \Rightarrow y^2 + x^7 + y^5 x^6 = 0$$

Picture of what is going on



What does blowing up do to these monomials? $y^n x^k$ doesn't change anything since we are going to change $y \rightarrow yx$ and then divide by x^n again.

In the case $y^{n-1} x^3 \rightarrow y^{n-1} x^{n-1+3} \rightarrow y^{n-1} x^{-1+3}$, so these kind of monomials go one step to the left, likewise any monomial whose power of y is less than n are shifted to the left and any monomial whose power of y is greater than n to the right.

So we can just keep blowing up and shift monomials to the left until one of them hits the blue line (the line $y^{n-i} x^i$), then we are back as in our first case, where we reduce multiplicity by blowing up.

This almost works but there is one problem. If we do this the monomials of degree n might be another n th power, it is not clear that this process terminates.

We keep doing transformations of the form $y \rightarrow y + *x^n$, for $n = 2, 3, 4, \dots$. There are two possibilities:

1. We keep going through this process an infinite amount of times.
2. This stops. We get an expression where we have a term in y^n , the term in $y^{n-1}x$ is zero and we have some non-zero terms under that in $y^{n-i}x^i$. But at this point we are done since

$$(y + \alpha x)^n = y^n + n\alpha y^{n-1}x + \dots$$

And $n\alpha \neq 0$ in char 0.

What if we get an infinite number of substitutions $y \rightarrow y + *x^n$? If this happens we find an infinite power series. The substitution

$$y \rightarrow y^n + *x^2 + *x^3 + \dots$$

transforms our polynomial to a power series $y^n +$ terms in $y^{\geq n}$, so our original polynomial is divisible by some (power series) n , where $n \geq 2$. But this is not possible as the original polynomial $f(x, y)$ has no multiple factors.

Remark. This can happen with polynomials with multiple factors, for example with the polynomial $f(x, y) = (y^2 - y + x^2)^2$, we can never resolve the singularities. A reason for this is that this polynomial has singularities at every point since it is a power of a nontrivial polynomial.

□

33.1 Newton's rotating ruler

Let start by taking $f(x, y) \in \mathbb{C}[x, y]$ such that f is not a polynomial in x . The result that Newton proved is that we can write y as a power series in $x^{1/N}$ for some N .

Definition 33.1. Puiseux Series

$$\bigcup_N \mathbb{C}[[x^{1/N}]] [x^{-1/N}]$$

They were first used by Puiseux in 1850, and first used by Newton in 1676.

Example 33.1.1. If $f(x, y) = y^2 - x^2 - x^3$, then:

$$y = x\sqrt{1+x} = x\left(1 + \frac{1}{2}x - \frac{1}{8}x^2 + \text{cdots}\right)$$

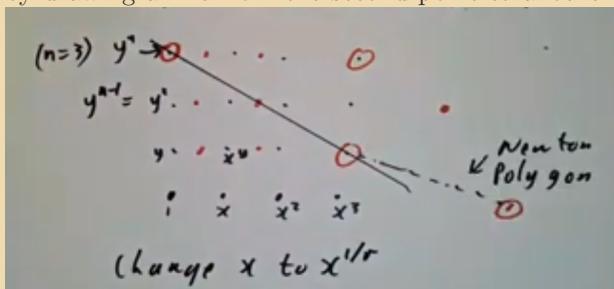
Another more trivial example:

If $f(x, y) = y^2 - x^3$; then $y = x^{3/2}$ which is a power series in $x^{1/2}$.

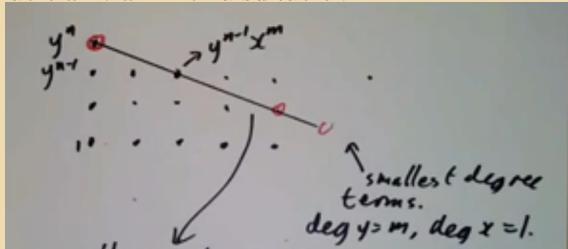
Theorem 24. Newton's theorem We can find solutions to algebraic equations that have power series in some fractional power of x .

Proof. We can assume $f(x, y)$ has a term y^n but not y^i for ($i < n$) (if everything in f is divisible by x we divide and continue). Then we plot all monomials $x^i y^i$ in f and mark the ones that occurs in f .

Then we take our ruler and rotate it until we can draw a line between y^n and a marked point, and we can continue by drawing a line from the second point to another marked point etc. The polygon we get is called a **Newton polygon**.



Then we add extra points, so that our line passes through a point on the line y^{n-1} , we do this by making a change of variable $x \rightarrow x^{1/r}$ for a suitable r .



We think of the points on the line as the smallest degree terms, where $\deg y = m$ and $\deg x = 1$. These monomials on the line form a homogenous polynomial in y, x^m . We factorize it to

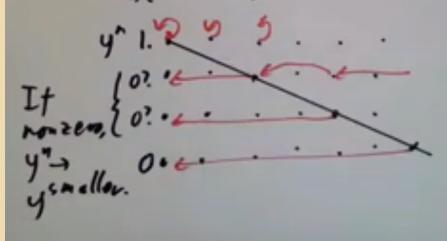
$$(y - \alpha x^m)(y - \beta x^m) \cdots$$

We do a change of variable $y \rightarrow y + \alpha x^m$

$$y(y - *x^m) \dots$$

What this means is that there is no term in x^{mn} . So 0 is a root possibly of high multiplicity.

Now we do a change of variable $y \rightarrow x^m y$, and all our terms are now divisible by x^{mn} , so we can divide by x^{mn} . So what happens to our coefficients? All the coefficients on the Newton ruler line are shifted.



If any of the coefficients as marked in the picture are non-zero we have changed $y^n \rightarrow y^{smaller}$, so we can go back and start again, with the smaller power of y .

This happens if the original root α is of multiplicity less than n . What do we do if it has multiplicity equal to n ? Then after the change of variable all the coefficients on Newton's ruler are zero, so we rotate it until we reach a new non-zero point.

This either continues forever or we reduce the smallest power of y ,
 this happens only a finite number of times

So we eventually reach where we change

$$y \rightarrow y + *x + *x^2 + \dots$$

So the coeffs $y^i x^i$, with $i < n$ are now zero.

So our series is divisible by y . So the *original* $f(x, y)$ is divisible by $(y - \text{power series in } x^{1/r})$, for some r

So we have found

$y = \text{power series in } x^{1/r}$

Such that $f(x, y) = 0$.

□

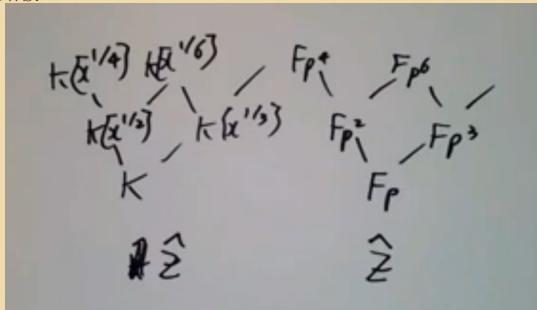
Consequences

Corollary 24.1. *The Field of Puiseux series is algebraically closed.*

Proof. Use Newton's method $f(x, y)$ which is a Puiseux series in x . We can think of this as a polynomial in $K[y]$, where K is the field of Puiseux series. So if we have a polynomial in y whose coefficients are Puiseux series, then we can find a root that is also a Puiseux series. So this field is alg closed \square

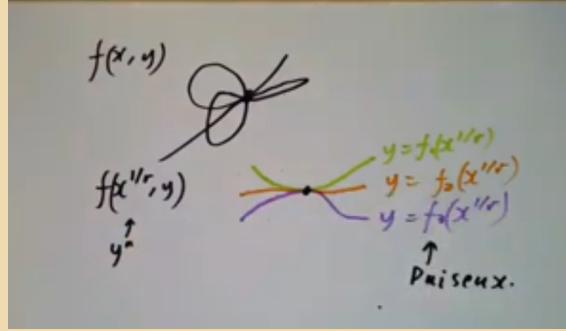
Definition 33.2. The Puiseux series are an example of a **Quasi finite field**. Which means that they behave like a finite field in the following sense.

The collection of field extensions of K are got by adding a root of x , this is similar to with finite fields as this diagram shows:



In both cases the “absolute Galois group” can be written as the completion of the integers, \mathbb{Z}

What does Newton's theorem have to do with resolutions of singularities? Suppose we have a plane curve $f(x, y)$ with singularities. Then Newton's theorem says that if we change $x \rightarrow x^{1/r}$. We have $f(x^{1/r}, y)$ which looks like this:



This is nearly a desingularisation of the singularity. We split off the singularity into a bunch of nonsing curves that touch at one point. We can “pull the curves apart” to resolve our singularity.

Lecture 8: Intersections

34 Hilbert Polynomials of graded modules over a graded ring

Suppose M is a graded module over a graded ring, i.e.

$$M = \bigoplus M_n \text{ and } R = k[x_1, \dots, x_n]/(I) \text{ where } \deg x_i = d_i > 0$$

We also take M to be finitely generated.

We can ask what is the “growth rate” of the components M_n ? We encode these dimensions as a function

$$f_M(x) = \sum x^n \dim(M_n), \text{ where } \dim M_n \text{ as a vector space over } k$$

Basic result: $f_M(x)$ is a *rational function*, we see this by looking at the following exact sequence:

$$0 \rightarrow \ker x_k \rightarrow M \xrightarrow{(1)} M(d_k) \rightarrow M(d_k)/x_k M \rightarrow 0$$

Where, $M(d_k)$ means M with a grading shifted by d_k and (1) is multiplication by x_k . Moreover $\ker x_k$ and $M(d_k)/x_k M$ are modules over R/x_k .

So

$$f_{M(d_k)} = x^{d_k} f_M \Rightarrow (1 - x^{-d_k}) f_M = \text{rational function}$$

Note the above function is indeed a rational function since it is something involving $\ker x_k$ and $M(d_k)/x_k M$ which are modules over rings with smaller number of generators so by induction are rational function.

Therefore f_M is a rational function! So

$$f_M = \text{rational function with denominators } (1 - x^{d_1})(1 - x^{d_2}) \cdots (1 - x^{d_k})$$

A special case is when all $d_i = 1$ the denom will be $(1 - x)^k$. We see that the coeffs of x^i for $i \geq 0$ are given by polynomials in i , for example

$$\begin{aligned} \frac{1}{1-x} &= 1 + x + x^2 + \cdots \\ \frac{1}{(1-x)^2} &= 1 + 2x + 3x^2 + \cdots \end{aligned}$$

Definition 34.1. This means that $\dim(M_n)$ is a polynomial in n for n large (> 0). This is called the **Hilbert Polynomial of M** . It describes how fast the graded pieces of M grow for large degree.

Special property of Hilbert polynomial In general the coefficients of this polynomial need not be integers, but this polynomial has the following property:

$$f(n) \text{ is an integer for } n \text{ integer}$$

So this is an integer valued polynomial. Since for any value of n (sufficiently large), this polynomial will be the dimension of some graded piece of M , and if a polynomial is a polynomial for large integer values then it is for all integer values.

What do integer valued polynomials look like? Well it is clear that $a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}$ if $x \in \mathbb{Z}$ and $a_i \in \mathbb{Z}$. But the converse is not true:

$$\frac{x(x-1)}{2} \in \mathbb{Z} \text{ for } x \in \mathbb{Z}$$

But it doesn't have integer coefficients.

Let us classify the integer valued polynomials:

$$\begin{aligned} 1 &= \binom{x}{0} \\ x &= \binom{x}{1} \\ \frac{x(x-1)}{2} &= \binom{x}{2} \\ \frac{x(x-1)(9x-2)}{3!} &= \binom{x}{3} \end{aligned}$$

Proposition 3. We claim that the binomial coefficients span all integer valued polynomials.

Proof. Suppose $f(n)$ is a degree k integer valued polynomial, we can find a linear combination:

$$f(n) - a_0 \binom{x}{0} - a_1 \binom{x}{1} - \dots - a_k \binom{x}{k} = 0$$

For $x = 0, 1, \dots, k$. We can do this since we can choose a_0 to make this polynomial vanish at $x = 0$, then we can choose a_1 such that this polynomial vanishes at $x = 1$, and since $\binom{x}{k}$ vanishes at $x = 0$ for $k > 1$ it will not affect the value of our polynomial at $x = 0$. And so on and so on....

So we get a polynomial of degree k vanishing at $k + 1$ points $(0, \dots, k)$ so it is 0 for all n . So we indeed see that any integer valued polynomial is a linear combination of binomial coefficients polynomials. \square

Important special case The leading coefficient of f is of the form

$$a_k \frac{x^k}{k!}$$

Where $a_k \in \mathbb{Z}$. This integer will turn out to give us the degree of various algebraic varieties.

34.1 Application: Degree of a variety

Suppose we have a projective variety $V \subseteq \mathbb{P}^n$, if V is a hypersurface then it would be given by $f(x_0, \dots, x_n) = 0$ and we can set

$$\deg V = \deg f$$

What if $\text{codim} > 1$? Notice that in the above case $\deg(V) = \#$ of intersection points of V with H (hypersurface), most of the time. Indeed if we take V to take a line and the hypersurface to be the same line then it would have infinite amount of intersection point instead of the usual 1.

So we say that the degree of V is the number of intersection points of V with a “generic” hyperplane. What does generic mean? It is not precisely defined, a hyperplane is generic if it makes things “work properly”.

Definition 34.2. In all cases for any variety V :

$$\deg(V) = \# \text{ intersection points with a LINEAR VARIETY of codim equal to } \dim V$$

Note a linear variety is: a line, plane, hyperplane, etc

This was the old and classical definition of a variety, which is fine for informal arguments but is tedious when we try to prove things.

Cleaner definition with Hilbert polynomial

Definition 34.3. The variety V corresponds to an ideal $I \subseteq k[x_0, \dots, x_n] = R$ (where $V = \text{zeroes of } I$). Since R/I is a graded ring it is a module over itself and so we get a Hilbert polynomial.

Recall that the degree of the Hilbert polynomial is equal to the $\dim V$ (This comes from commutative alg, where we have a theorem that says \dim of a local ring $= 1 + \deg$ Hilbert poly of a graded ring m^n/m^{n+1}). As we saw last lecture the leading coefficient of the Hilbert polynomial is $a \frac{x^d}{d!}$, for some integer a . This integer a is called the **degree** of V

Example 34.3.1. Let $V = \mathbb{P}^n$, then we take the graded ring $k[x_0, \dots, x_n]$ and $I = 0$.

We look at the graded pieces of this graded ring. There are 1 thing of degree 1, there are $\frac{n(n-1)}{2}$ things of degree 2... In general we see that we have

$$\binom{n+k}{n} = \frac{k^n}{n!} + \text{smaller terms}$$

So we have $\dim(\mathbb{P}^n) = n$ and $\deg(\mathbb{P}^n) = 1$.

Hypersurface of degree d polynomial $f(x_0, \dots, x_n)$

Example 34.3.2. We are looking at the graded ring $k[x_0, \dots, x_n]/(f)$. The Hilbert polynomial is:

$$\binom{n+k}{n} - \binom{n+k-d}{n} = \frac{dk^{n-1}}{(n-1)!} + \text{smaller terms}$$

We are taking the number of monomials of degree k and subtracting the monomials of degree $k-d$ (we subtract those since any of these times f will be of degree n).

So the hypersurface has dimension $n-1$, and the degree is d .

Twisted cubic $\subseteq \mathbb{P}^3$

Example 34.3.3. Recall that if we take the ring of polynomial to be $k[w, x, y, z]$, then the Twisted cubic is defined by the equations:

$$wz = xy, \quad x^2 = wy, \quad y^2 = xz$$

In general, we can kill off any terms containing x^2, y^2 or xy . Since we can turn them into smaller powers of x and y . So a basis of the quotient ring is

$$w^i z^{k-i}, w^i x z^{k-i-1}, w^i y z^{k-i-1} \text{ degree } k \geq 3$$

There are $k+1+k+k = 3k+1$ possibilities, so $\frac{3k}{1!} + 1$ is the Hilbert polynomial. So we see that degree is equal to three and has dimension equal to 1.

But recall that the twisted cubic is isomorphic to \mathbb{P}^1 , which has degree 1. So the degree is not an invariant, it depends on the embedding of the abstract variety into projective space.

Invariant of projective variety, the euler polynomial of V

Definition 34.4. We call

$$\chi(V) = \text{constant term of Hilbert polynomial}$$

The **Euler polynomial** of V .

Property 1: $\chi(V)$ depends only on the abstract variety V , not on the embedding into projective space

Definition 34.5. For historical reasons people would use

$$(-1)^{\dim}(\chi(V) - 1)$$

Which is called the **Arithmetic genus**

Property 2: $\chi(V \times W) = \chi(V)\chi(W)$. Which is not a property that the Arithmetic genus has.

Remark. When we do sheaf cohomology we will see that there is another definition of $\chi(V)$.

Working out arithmetic genus of plane curve, degree d

Example 34.5.1. The Hilbert polynomial:

$$\binom{2+k}{2} - \binom{2+k-d}{2} = 1 + dk - \frac{(2-d)(1-d)}{2}$$

So the arithmetic genus is $\frac{(2-d)(1-d)}{2}$, this is where the name comes from, for topological curves the arithmetic genus is the same as the topological genus.

The hilbert polynomial is more or less the only discrete invariant of closed subvarieties of projective space: Theorem by R. Hartshorne.

35 Bézout's theorem

In it's most simplest form **Bézout's theorem** says that "If we have two curves of degree m, n then they intersect in mn points". The problem is that this version of the theorem is false.

Problems with this theorem

1. They may have parallel lines, so they would intersect in zero points. In order to work around this we need to work in \mathbb{P}^2 (we need points at infinity).
2. If we take two curves like $y = 0$ and $y = x^2 + 1$, they intersect in no real points. We need to use an algebraically closed field (\mathbb{C} in our case)
3. They may have a component in common, in fact they may be the same curve. We need to say that they have no components in common.
4. Points may have multiplicities, for example $y = 0$ and $y = x^2$ only have one point in common, but we need to think of this intersection point as a point with multiplicity 2. If we deform the parabola slightly it meets the straight line at two points.

Theorem 25. One version of Bézout's theorem Two distinct irreducible curves in $\mathbb{P}^2(\mathbb{C})$ of degrees m, n repec. Intersect in mn points counted with multiplicities.

Note that we haven't stated what *multiplicity* is in this question.

Variations of Bézout's theorem

Theorem 26. n -dim version of Bézout's theorem n distinct hypersurfaces in $\mathbb{P}^n(\mathbb{C})$ of degrees d_1, \dots, d_n usually intersect at $d_1 \cdots d_n$ points.

Roughly speaking *usually* means that the intersection shouldn't have the wrong dimension.

Remark. Take two algebraic sets of degree m, n is their intersection of degree mn ?

We have the usual problem, that the intersection must be of the wrong degree.

Informal “proof” While an informal proof is not a proof this is a sort of intuition for it. “*Proof*”

$f(x, y) = 0$ and $g(x, y) = 0$. We deform f, g so they are both the union of a finite number of lines. Then f is the union of m lines and g is the union of n lines, so there are mn points of intersection.

QED?

This is not a proof, since we haven't shown that the number of interesection points doesn't change as we deform f, g .

How do we state and prove Bézout's theorem correctly?

Defining multiplicity We need to use the theory of finitely generated modules M over a Noetherian ring R .

We have:

$$0 = M_0 \subseteq M_1 \subseteq M_2 \dots \subseteq M_n = M$$

So that $M_i/M_{i-1} \simeq R/p$ for some prime ideal p . (*proof:* We choose I maximal among ideals such that $R/I \subseteq M$, it is easy to check that I is prime, and let $M_1 \simeq R/I$ and repeat for M/M_1)

Definition 35.1. Phoney definition We define multiplicity of R/p in M to be the number of times R/p is isomomorphic to M_i/M_{i+1} .

The problem is that this definition doesn't work in general.

Example 35.1.1. An example where this works Let $R = \mathbb{Z}$, and M = a finite group. Then:

$$R/(p) = \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \dots$$

So the number of times $\mathbb{Z}/p_1\mathbb{Z}$ is in M is equal to n_1 , where $|M| = p_1^{n_1} p_2^{n_2} \cdots$

Example 35.1.2. However if M is f.g. this might not be well defined. If $M = \mathbb{Z}$, then we have:

$$\underbrace{0}_{M_0} \subseteq \underbrace{\mathbb{Z}}_{M_1} \text{ then } \mathbb{Z}/2\mathbb{Z} \text{ occurs 0 times}$$

But we can take another filtration of \mathbb{Z} :

$$\underbrace{0}_{\simeq \mathbb{Z}/(0)} \subseteq \underbrace{2\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}} \subseteq \mathbb{Z} \text{ then } \mathbb{Z}/2\mathbb{Z} \text{ occurs once}$$

So we can't define multiplicity in \mathbb{Z} , it varies depending on what filtration we use.

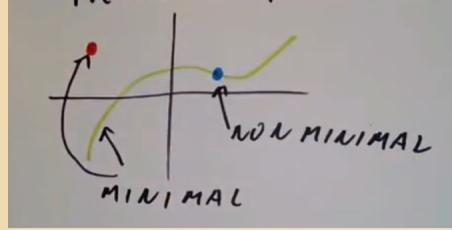
Example 35.1.3. M is a f.g. module over \mathbb{Z} , the multiplicity of $\mathbb{Z}/(0)$ in M is defined.

Sometimes the multiplicity is not defined, and sometimes it is defined what is the difference?

Remark. Look at prime ideals p_1, p_2, \dots with R/p_i in a filtration of M . If p_i is *minimal* in this set, we get a well-behaved multiplicity.

Indeed if p_i minimal, the multiplicity is equal to the length of M_p over R_p where R_p is the localization of R at p .

Geometric way of looking at this Let $R = \mathbb{C}[x, y]$; prime ideals correspond to points, curves and the plane. Suppose we have a picture like this:



The multiplicity of the red and green primes are well-defined but not of the blue prime. Furthermore recall that while the blue prime seems smaller than the green one, the order gets reversed when we look at ideals.

To summarise, if we have a module over a ring R , we can define the multiplicity for some primes of R .

There is a similar theorem for graded modules over graded rings, the only difference is that if we have a graded prime we might have to shift the degree of everything by some integer ℓ denoted like this $(R/p)(\ell)$

Finally, Bézout's theorem

Theorem 27. Let Y be a variety in \mathbb{P}^n and take H , a hypersurface given by $f(x_0, \dots, x_n) = 0$. We assume that Y is not contained in H .

Then

$$\sum_j i(Y, H; Z_j) \deg Z_j = \deg Y \deg H \quad (\dagger)$$

Here $Y \cap H$ is the union of irreducible components of Z_j and $i(Y, H; Z_j)$ is the multiplicity of Y and H at Z_j .

We look at the following exact sequence

$$0 \rightarrow k[x_0, \dots, x_n] / I_Y \xrightarrow{\cdot f} k[x_0, \dots, x_n] / I_y \rightarrow k[x_0, \dots, x_n] / (I_y, f) \rightarrow 0$$

Note when we multiply by f , we must shift the degree by $-\deg f$.

Now the hilbert polynomial of (2) – the hilbert polynomial of (1) = hilbert polynomial of (3). So

Hilbert polynomial of (3) = $p_Y(z) - p_Y(z - d)$ note we subtract by d since we shifted the degrees

So the hilbert polynomial is

$$\frac{\deg Y Z^{\dim Y}}{(\dim Y)!} + \dots - \frac{\deg Y (Z - d)^{\dim Y}}{(\dim Y)!}$$

Since $(Z - d)^{\dim Y} = Z^{\dim Y} - \dim Y \cdot d Z^{\dim Y - 1}$; the leading term of our hilbert polynomial is:

$$d \deg Y \frac{Z^{\dim Y - 1}}{(\dim Y - 1)!}$$

The conclusion is

Hilbert polynomial of $k[x_0, \dots, x_n] / (I_y, f)$ has leading term of $\deg H \deg Y \frac{Z^{\dim Y - 1}}{(\dim Y - 1)!}$

Proving † Now the module $k[x_1, \dots, x_n]/(I_Y, f)$ has a filtration:

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n = M$$

Where the quotients are $(R_i/q_i)(\ell_i)$, for some prime ideal q_i . Shifting the the degree by ℓ_1 doesn't change the leading coefficient. So the Hilbert polynomial of each of these has leading coefficients

$$\frac{\deg Z_j}{(\dim Z_j)!} Z^{\dim Z_j}$$

Where $\dim Z_j = \dim Y - 1$

So we see that

$$\deg H \deg Y = \sum_i \deg Z_j \cdot \text{multiplicity of } (R/q_i) \text{ in } k[x_0, \dots, x_n]/(I, f)$$

So we need to show that multiplicity of (R/q_i) in $k[x_0, \dots, x_n]/(I, f)$ is the multiplicity of the intersection.

We need to use the *sharphooter technique™*, we define our target to be what we shot at i.e. We **define the multiplicity of the intersection** to be multiplicity of (R/q_i) in $k[x_0, \dots, x_n]/(I, f)$

Part 1 DONE!

□