Borcherd Algebraic Geometry 1

Rindra Razafy, "Hagamena"

August 1, 2022

Contents

0 Prologue

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

Lecture 1:

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

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

If we look at the equation mod 4 we notice that $x^2, y^2, z^2 \equiv 0, 1 \mod 4$, 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 rearange the equation:

$$y^2 = z^2 - x^2 = (z - x)(z + x) \tag{2}$$

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 $d \mid 2z$ and $d \mid 2x$, 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:

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

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

$$X^2 + Y^2 = 1, \ X, Y \text{rational} \tag{4}$$

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:

$$(x_1, y_1) \times (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \tag{5}$$

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:

$$(\cos\theta_1, \sin\theta_1) \times (\cos\theta_2, \sin\theta_2) = (\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2, \dots) = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)) \tag{6}$$

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.

$$G\colon R \to (\{(x, y) \in R^2 \mid x^2 + y^2 = 1\}, \times) \tag{7}$$

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

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

Summary There are many ways to view a circle:

1. Subset of $\mathbb{R}^2$
2. Polynomial $x^2 + y^2 - 1 \to$ 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 cubes.

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:

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

   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 Singluarity 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:

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

   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: $a_1 + a_2 + \cdots = b_1 + b_2 + \cdots \iff$ 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 anologue of Bézout's theomre 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 anologuous result in a plane over a division ring then:

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

3.3 Pascal's theorem

Theorem 3. *Informally: Choose any six points on an ellipse, seperate 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.*

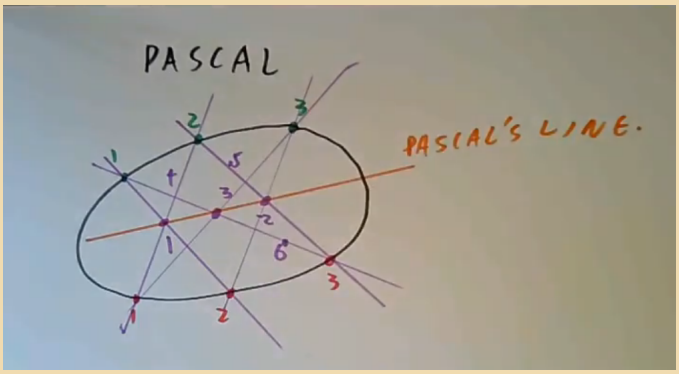


Illustration from the lecture video

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

Pappus' theorem is a degenerate case of Pascal's theorem, Pascal's theorm 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 $i \in \{1, \ldots, 6\}$ where $p_i = 0$ on line i.

Now look at $p_1p_3p_5$ and $p_2p_4p_6$, these polynomials vanish on all six points, so choose λ such that:

$$p_1p_3p_5 - \lambda p_2p_4p_6 \text{ this is of degree 3 curve} \tag{1}$$

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 $p_1p_3p_5$ and $p_2p_4p_6$ both vanish on the three intersection points, since they are on the curve but not on the conic, they must be on the line. □

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 triange.

Slight variation of the defintion, is that it is a set contianing 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 $f = 0$. □

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

Note there is an obvious line:

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

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:

5 Affine space and Zariski topology

5.1 Affine space

Definition 5.1. Let k be any field (most commononly 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:

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

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 "forgotting" 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:

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

Indeed a homomorphism taking $k[x_1, \dots, x_n] \to k$, just takes $x_i \to a_i$ 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 algebric 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 $\{f_i g_j\}$
- 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 $\mathbb{A}^{mn}$ = linear maps $k^m \to k^n = m \times n$ 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 partucular the subset of maps from $k^m \to k^n$ 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,$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, is eventaully 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 $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, of R where:

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

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

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

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

Note the sets s_i are finite since R is Noetherian.

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

Corollary 4.1. ***Hilbert***

$k[x_1, \ldots, x_n]$ 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 $k[x_1, \ldots, x_n]$ is Noetherian. □

6.2 Noetherian spaces

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

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

  $$C_0 \supseteq C_1 \supseteq C_2 \supseteq \ldots$$

  Stabilises, i.e. $C_n = C_{n+1} = \ldots$, 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 $k[x_1, \ldots, x_n]$. A descsending chains of closed sets of $\mathbb{A}^n$ correspond to an ascending chain of ideals in $k[x_1, \ldots, x_n]$ □

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 regualar 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 somewhen 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. □

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.*

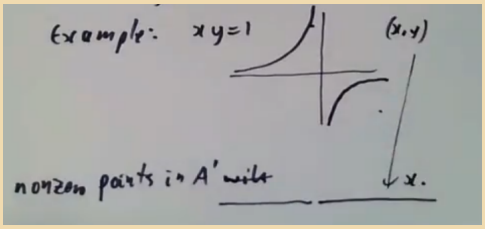
Definition 6.5. A provisional definition of Algebraic Varieties:

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 $(x, y) \to x$, we should consider it an algebraic variety.



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

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

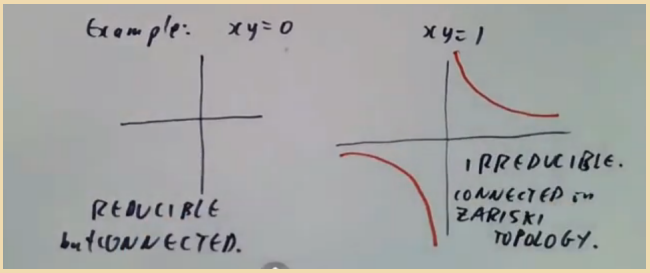
This is the union of four irreducible subsets:

1. $x = y = z$
2. $x = 0y = z$
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 $xy = 1$, the we 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 subsetes of the corresponding affine sets.

- If we have a subset $Y \subseteq \mathbb{A}^n$ we can map it to the ideal $I(Y) \subseteq k[x_1, \ldots, x_n]$ where $I(Y)$ is the set of polynomials vanishing on Y.
- If we have an ideal $\mathfrak{a} \subseteq k[x_1, \ldots, x_n]$ we can map it top 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 definiton of the Zariski topology, let W be any closed set contianing 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 $\mathfrak{a} \subseteq k[x_1, \ldots, x_n]$? **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

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

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

Is $\sqrt{a} = I(Z(\mathfrak{a}))$? 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 $k[x_1 m \dots, x_n]$ 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 $\sum_{k=1}^n \frac{a_k}{x - a_k} = 0 \Rightarrow \sum_{k=1}^n a_k \prod_{i \neq k}(x - a_j) = 0$, 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. □

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 finietely 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 $I \neq k[x_1, \dots, x_n]$. □

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 $I(Z(\mathfrak{a})) = \sqrt{a}$.*

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 $\mathfrak{A}^{n+1}$, 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 $\mathbf{A}^{n+1}$, 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:

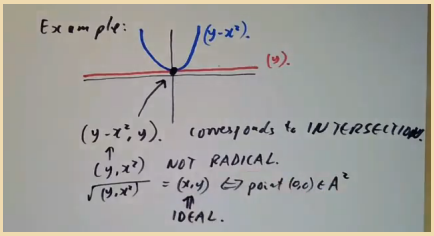
$$f^n = \sum h_i f_i \text{ where } h_i = f^n g_i \in k[x_1, \dots, x_n]$$

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

Affine space $\mathbb{A}^n$	correspondence	$k[x_1, \ldots, x_n]$
Points $(a_1, \ldots, a_n)$	$\overset{\iff}{\underset{WeakNullstellensatz}{}}$	maximal ideals $(x_1, \ldots, x_n)$
Algebraic sets	$\overset{\iff}{\underset{StrongNullstellensatz}{}}$	Radical ideals $\mathfrak{a} = \sqrt{\mathfrak{a}}$
closed subschemes	$\overset{\iff}{\underset{Will\ see\ in\ second\ part\ of\ course}{}}$	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:

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

The entries of the matrix A^n generate an ideal I in the coordinate ring of 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 $a_{11} + a_{22} + \cdots + a_{nn} \notin I$, 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 $\mathrm{tr}(A) = a + d$ 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 $(a + d)^3$.

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

$$(a+d)^3 = a^3 + 3a^2d + 3ad^2 + d^3 \tag{1}$$

What about communting 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.

Lecture 3:

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 $k[x_1 \ldots, x_n]$ 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 isomomorphic 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:

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

- *A more convinent 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: $M \subseteq \oplus_{finite}$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 interesection of itself, or it is the intersection of two larger submodules which are by induction a finite intersection of irreducibles, contradiction. □

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 irreducibles. □

Combining the two previous lemmas gives us our proof. □

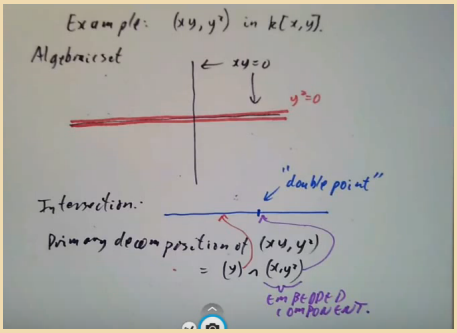
Example 8.3.3. Let us look at the ideal generated by (xy, y^2) in $k[x, y]$.

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

The intersection of these two sets is just the x-axis, whith 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 it's coordinates ring $k[x_1, \ldots, x_n]/I(Y)$, 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 $f + I(Y) \to f|_Y$. This is well definied 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 $\omega(x_1, \ldots, x_n) = \sum_i a_i m_i(x_1, \ldots, x_n)$, for some monomial m_i. So we just need to set $f = \sum_i a_i m_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$.

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 properites, 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 properites. In technical terms the category of algebraic sets is equiv to opposit 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.

$$\text{So we can look at the } \textbf{Ring of invariant } \Big(k[x_1,\dots,x_n]/I(Y)\Big)^G.$$

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 finietely generated were found after him.

Example 9.0.1. Let $\mathbb{A}^n$ = 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**:

- $p_1 = x_1 + \cdots + x_n$
- $p_2 = x_1x_2 + \cdots$
- $\vdots$
- $p_n = x_1 \dots x_n$

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 $x \to -x$, 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:

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

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 $a_nx^n + a_{n-1}x^{n-1}y + \cdots + a_0y^n$, 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 $a_2x^2 + a_1xy + a_0y^2$, the invariant is the **discriminant** which is $a_1^2 - 4(a_0a_2)$

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 fintieness 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 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

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

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 $k^n = span\{x_1, \dots, x_m\}$ so G acts on A. Let A^G =invariant elements of A. A^G is finitely generated as a k-algebra if G is finite and chark $= 0$.*

Proof. Notice that A is graded by degree:

$$A = A_0 \oplus A_1 \oplus A_2 \dots \tag{2}$$

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 =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 sho they genereate 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:

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

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

By properties of the Reynold 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. □

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

Extensions of this thorem

1. For G compact and $k = \mathbb{R}$ or $\mathbb{C}$, the same proof works since we can define a Reynods 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 finietely general.

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

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

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

So in reality the ring of invariant is equal to

$$k[z_0, \ldots, z_4]/(z_1 z_2 = z_0 z_3, {z_1}^2 - z_0 z_2, {z_2}^2 - z_1 z_2) \tag{†}$$

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

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 chemestry 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:

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

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:

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

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 tbat is topologically isomorphoic 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 $\lambda \to \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}$ These six transformations form a group isomorphic to S_4.

So we have an affine variety given by

$$(\mathbb{A}^1 \setminus \{0, 1\})/S_3 \tag{†}$$

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 †? 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:

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

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.