Lectures on Algebraic Groups

Dipendra Prasad

Notes by Shripad M. Garge

1. Basic Affine Algebraic Geometry

We begin these lectures with a review of affine algebraic geometry.

Let k be an algebraically closed field. An *Affine algebraic variety* over k is a subset $X \subseteq \mathbb{A}^n := k^n$ of the form

$$X = \big\{x \in \mathbb{A}^n : f_i(x) = 0 \text{ for certain } f_1, \ldots, f_r \in k[x_1, \ldots, x_n]\big\}.$$

Thus, an affine algebraic variety is the set of common zeros of certain polynomial equations. The *coordinate ring* of an affine variety X, denoted by $k[X]$, is the ring of polynomial functions on X; it is given by

$$k[X] := \frac{k[x_1, \ldots, x_n]}{\sqrt{(f_1, \ldots, f_r)}},$$

where for an ideal I, we define

$$\sqrt{I} = \big\{g \in k[x_1, \ldots, x_n] : g^m \in I \text{ for some } m \geq 0\big\}.$$

The notions of subvariety and a finite product of varieties make sense and are defined in the most natural way.

If $X \subseteq \mathbb{A}^n$, and $Y \subseteq \mathbb{A}^m$ are affine algebraic varieties, then by a *polynomial map* from X to Y, we mean a mapping from X to Y which is the restriction to X of a mapping from $\mathbb{A}^n$ to $\mathbb{A}^m$ given by

$$(x_1, \ldots, x_n) \longmapsto \big(\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n)\big)$$

with $\phi_i \in k[x_1, \ldots, x_n]$.

The map $X \longmapsto k[X]$ defines a natural contravariant transformation. Clearly a polynomial map $f : X \longrightarrow Y$ gives rise to a map from $f^* : k[Y] \longrightarrow k[X]$ defined by, $f^*(\phi) = \phi \circ f$.

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, dashed, "f^*(\phi)"'] & Y \arrow[d, "\phi"] \\
 & k
\end{tikzcd}$$

It is obvious that such a function on X is given by a polynomial function.

Theorem. *There exists a functorial correspondence between affine algebraic varieties and finitely generated k-algebras without nilpotents. This correspondence is contravariant.*

One defines a topology on an affine algebraic variety X by taking closed sets of X to be zeros of polynomials. It is called as the *Zariski topology* on X.

If $X_1 \subseteq X$ and $X_2 \subseteq X$ are closed subsets then $X_1 \cap X_2$ and $X_1 \cup X_2$ are closed. Indeed, if X_1, X_2 are given by $\{f_\alpha\}, \{g_\beta\}$ respectively, then $X_1 \cap X_2$ and $X_1 \cup X_2$ are given by $\{f_\alpha, g_\beta\}$ and $\{f_\alpha g_\beta\}$ respectively.

One important difference between the Zariski topology and the usual metric topology is that the Zariski topology is not Hausdorff. This can be seen already for $X = \mathbb{A}^1$. Here the closed sets are precisely all subsets of finite cardinality besides the whole set X. Thus non-empty open sets are complements of finite sets. Therefore any two non-empty open sets intersect, and hence the space $\mathbb{A}^1$ is not Hausdorff with the Zariski topology.

Proposition. *Let X be an algebraic variety.*

(i) *Any family of closed subsets of X contains a minimal one.*

(ii) *If $X_1 \supset X_2 \supset \ldots$ is a descending sequence of closed subsets of X, then there exists k such that $X_i = X_k$ for all $i \geq k$.*

Proof. The proof follows as the polynomial algebra $k[x_1, \ldots, x_n]$ is Noetherian. $\square$.

The property (i) in the above proposition states that an algebraic variety is *Noetherian* with the Zariski topology. Note that the two properties in the above proposition are equivalent!

An *irreducible algebraic variety* is the one in which any two non-empty open sets intersect. Example: $\mathbb{A}^1$ is irreducible.

An algebraic variety is irreducible if and only if any non-empty open set is dense in it. A subvariety is irreducible if it is irreducible in the induced topology. Following statements are easy to prove.

Lemma.

(i) *A subvariety Y of an algebraic variety X is irreducible if and only if $\overline{Y}$ is irreducible.*

(ii) *If $\phi : X \longrightarrow Z$ is a morphism and X is irreducible, then so is $\phi(X)$.*

(iii) *If X_1, X_2 are irreducible varieties, then so is $X_1 \times X_2$.*

Note that an irreducible algebraic variety is always connected but the converse is not true. Example: Take $X = \{(x, y) \in \mathbb{A}^2 : xy = 0\}$. Here the open sets, viz., $Y_1 = \{(x, 0) \in X : x \neq 0\}$ and $Y_2 = \{(0, y) \in X : y \neq 0\}$ do not intersect each other. And $X = \{(x, 0)\} \cup \{(0, y)\}$, where both the sets $\{(x, 0)\}$ and $\{(0, y)\}$ are connected (being homeomorphic to $\mathbb{A}^1$) and they intersect each other, hence the union is connected.

The geometric intuition behind the irreducible variety is that a general variety is a finite union of "components" where a component means a maximal irreducible subset.

Irreducible varieties correspond to minimal elements in the primary decomposition of the ideal (0) in the coordinate ring $k[X]$. A variety X is irreducible if and only if the corresponding coordinate ring $k[X]$ is an integral domain.

Let X be an irreducible variety. Let $k(X)$ denote the field of fractions of the integral domain $k[X]$. This is the field of meromorphic functions on the variety X. We define *dimension* of the irreducible variety X to be the transcendence degree of $k(X)$ over k. Dimension also equals the length of maximal chain of irreducible subvarieties.

Examples:

(i) $\mathbb{A}^1 : \{0\} \subset \mathbb{A}^1,\ \dim(\mathbb{A}^1) = 1;$

(i) $\mathbb{A}^2 : \{0\} \subset \mathbb{A}^1 \subset \mathbb{A}^2,\ \dim(\mathbb{A}^2) = 2.$

For a general variety X, the dimension is maximal of dimensions of its irreducible components.

Lemma. *Let X, Y be irreducible varieties of dimensions m, n respectively, then $\dim X \times Y = m + n$.*

Proof. This is clear since $k[X \times Y] = k[X] \otimes k[Y]$. □.

Lemma. *Let X be an irreducible variety and let Y be a proper subvariety of X. Then $\dim Y < \dim X$.*

Proof. Let $k[X] = k[x_1, \ldots, x_r]$ and $k[Y] = k[X]/P$, where P is a nonzero prime ideal. Let y_i be the image of x_i in $k[Y]$. Let $\dim X = m$ and $\dim Y = n$. We can assume that $y_1, \ldots, y_n$ are algebraically independent. Then clearly $x_1, \ldots, x_n$ are algebraically independent, hence $m \leq n$. Assume that $m = n$. Let f be a nonzero element of P. Then there is a nontrivial relation $g(f, x_1, \ldots, x_n)$ where $g(t_0, \ldots, t_n) \in k[t_0, \ldots, t_n]$.Since $f \neq 0$, we can assume that t_0 does not divide all monomials of g, hence $h(t_1, \ldots, t_n) := g(0, t_1, \ldots, t_n)$ is nonzero, but then $h(y_1, \ldots, y_n) = 0$ contradicting the algebraic independence of y_i. This completes the proof. □.

A *locally closed set* is an open subset of a closed set. Example: $\mathbb{A}^* \hookrightarrow \mathbb{A}^2$ as the subset $\{(x, 0) : x \in \mathbb{A}^*\}$, is locally closed.

A *constructible set* is a finite union of locally closed sets. Example: $\mathbb{A}^2 - \mathbb{A}^* \hookrightarrow \mathbb{A}^2$ is constructible but not locally closed.

Theorem. (Chevalley). *If $f : X \longrightarrow Y$ is a morphism of algebraic varieties, then $f(X)$ is constructible.*

Example: Let $f : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ be the morphism given by $f(x, y) = (x, xy)$. Then $f(\mathbb{A}^2) = \mathbb{A}^2 - \mathbb{A}^*$.

We shall also need the notion of projective varieties. These are the varieties that are defined by homogeneous polynomials. These varieties can be seen as closed subsets of $\mathbb{P}^n$ for some n, hence the name projective.

2. Affine Algebraic Groups

An *affine algebraic group* G is an affine algebraic variety as well as a group such that the maps $m : G \times G \longrightarrow G$ and $i : G \longrightarrow G$, given by $m(x, y) = xy, i(x) = x^{-1}$, are morphisms of algebraic varieties.

Examples of affine algebraic groups:

(i) Any finite group can be made into an algebraic group. To make G into an algebraic group, we have to give a finitely generated k-algebra $k[G]$. We take $k[G]$ as the algebra of functions on G.

(ii) The groups $GL_n, SL_n, Sp_{2n}, SO_n, O_n, U_n$, etc. are some of the standard examples of affine algebraic groups.

For the group GL_n, the structure of an affine algebraic group is given by,

$$GL_n = \left\{ \begin{pmatrix} X & 0 \\ 0 & x_{n+1} \end{pmatrix} : \det X \cdot x_{n+1} = 1 \right\}.$$

The multiplication $m : GL_n \times GL_n \longrightarrow GL_n$ is a polynomial map, $(X)_{ij} \cdot (Y)_{ij} \longmapsto (Z)_{ij}$. To say that the map m is polynomial is equivalent to say that coordinates of Z depend on those of X and Y polynomially.

As a special case, for $n = 1, GL_1 = \mathbb{G}_m = k^*$ and the coordinate ring is $k[GL_1] = k[x][x^{-1}]$.

Lemma. *A closed subgroup of an algebraic group is an algebraic group.*

Proof. Clear from the definitions. □

Remark. A locally closed subgroup is closed. In fact every open subgroup is closed. (Hint: Coset decomposition)

This remark is not true in the case of topological groups. Example: A line with irrational slope in $\mathbb{R}^2$, gives an embedding of $\mathbb{R}$ into $\mathbb{R}^2/\mathbb{Z}^2$ as an everywhere dense subgroup of the torus $\mathbb{R}^2/\mathbb{Z}^2$.

Lemma. *Let $\phi : G_1 \longrightarrow G_2$ be a homomorphism of algebraic groups then $\phi(G_1)$ is a closed subgroup of G_2.*

Proof. From Chevalley's theorem, $\phi(G_1)$ is constructible. We can assume without loss of generality, that $\phi(G_1)$ is dense in G_2.

Since $\phi(G_1)$ is constructible, it contains an open subset of G_2, hence $\phi(G_1)$ is open in G_2. And then by previous remark $\phi(G_1) = G_2$. This completes the proof. □

Lemma. *A connected algebraic group is irreducible.*

Proof. One needs to prove that there is a unique irreducible component of G passing through $\{e\}$, the identity of the group G. Let $X_1, \ldots, X_m$ be all irreducible components of G passing through $\{e\}$.

Look at the mapping $\phi : X_1 \times \cdots \times X_m \longrightarrow G$, given by multiplication. Since X_i are irreducible, so is their product and also the image of the product in G under the map ϕ. Clearly the image contains identity and therefore the image of the map ϕ is contained in an irreducible component of G, say X_1. Since all X_i contain identity, this implies that all X_i are contained in a fixed X_1. □

Lemma. *The irreducible component of G passing through $\{e\}$ is a closed normal subgroup of G of finite index.*

Proof. We denote the irreducible component of G passing through $\{e\}$ by G°. Being closed is a general property of irreducible algebraic varieties, hence G° is closed in G. To prove that G° is a subgroup of G, we must show that whenever $x, y \in G^\circ$, $xy^{-1} \in G^\circ$. Clearly $x^{-1}G^\circ$ is also irreducible and $e \in x^{-1}G^\circ \cap G^\circ$, thus $x^{-1}G^\circ = G^\circ$, i.e., $x^{-1}y \in G^\circ \ \forall\, x, y \in G^\circ$. Similarly one can prove that G° is normal.

An algebraic variety has finitely many irreducible components, hence G° is of finite index in G. This completes the proof. □

Lemma. *For an algebraic group G, any closed subgroup of finite index contains G°.*

Proof. Let H be a subgroup of G of finite index. Then H° is closed and hence open in G° (being a subgroup of finite index), hence $H^\circ = G^\circ$.

Remark. If n is odd, then there is no real difference between $SO(n)$ and $O(n)$ as $O(n) = \{\pm 1\} \times SO(n)$.

$$0 \longrightarrow SO(n) \longrightarrow O(n) \longrightarrow \mathbb{Z}/2 \longrightarrow 1$$

$$0 \longrightarrow (\mathbb{Z}/2)^{n-1} \longrightarrow W(SO(2n)) \longrightarrow S_n \longrightarrow 1$$

$$0 \longrightarrow (\mathbb{Z}/2)^{n} \longrightarrow W(SO(2n+1)) \longrightarrow S_n \longrightarrow 1$$

3. Group Actions on Algebraic Varieties

Let G be an algebraic group, and X an algebraic variety. A *group action* of G on X is a morphism of algebraic varieties $\phi : G \times X \longrightarrow X$ such that $\phi(g_1, \phi(g_2, x)) = \phi(g_1 g_2, x)$ and $\phi(e, x) = x, \ \forall\, g_1, g_2 \in G, x \in X$.

An algebraic variety X is called *homogeneous* if G operates transitively on X. Isotropy subgroups, orbits are defined in the natural way.

Lemma. *Isotropy subgroups are closed. Orbits are open in their closure.*

Proof. The map $\phi : G \times X \longrightarrow X$ gives rise to a map $\phi_1 : G \longrightarrow X \times X$ defined by, $g \overset{\phi_1}{\longmapsto} (x_0, gx_0)$ for a fixed $x_0 \in X$. Then the isotropy subgroup of x_0, viz. G_{x_0} is the inverse image of (x_0, x_0) under the map ϕ_1 and hence is closed.

G operates on X, $Gx_0 \subseteq X$. In fact, $Gx_0 \subseteq \overline{Gx_0} \subseteq X$. The set Gx_0 is constructible, i.e., contains an open subset U of $\overline{Gx_0}$, and Gx_0 is union of the cosets $gU, g \in Gx_0$, therefore Gx_0 is open in $\overline{Gx_0}$. □

Lemma. *For any group action $\phi : G \times X \longrightarrow X$, there is always a closed orbit in X.*

Proof. It suffices to prove the lemma under the condition that G is irreducible because if Z is a closed orbit under the action of G°, then $G \cdot Z$ is a finite union of closed sets, and hence is closed, and Z being an orbit of G°, $G \cdot Z$ is an orbit of G. So, we now assume that G is irreducible.

Choose an orbit whose closure has smallest dimension, say Gx_0. Write $\overline{Gx_0} = Gx_0 \cup Y$. As Gx_0 is G invariant, so is $\overline{Gx_0}$ and hence Y is also G invariant, then $\dim Y < \dim \overline{Gx_0}$ and Y is closed. Contradiction! □

Some standard contexts for group action:

(i) G acts on itself via left and right translations, and this gives rise to an action of $G \times G$ on G, given by, $(g_1, g_2) \cdot g = g_1 g g_2^{-1}$. This is a transitive action, the isotropy subgroup of identity being $\Delta G \hookrightarrow G$.

(ii) If V is a representation of G, then this gives an action of G on V, and one may classify orbits on V under this action.

Exercise 1. The group $G = GL_n$ operates on $V = \mathbb{C}^n$ in the natural way. Classify orbits of G action on $\mathrm{Sym}^2(V)$ and $\wedge^2(V)$ induced by this natural action.

Answer. Action of GL_n on $\mathrm{Sym}^2(V)$ is essentially $X \longmapsto gX^t g$. Number of orbits in V is 2, in $\mathrm{Sym}^2(V)$ it is $n+1$ and in $\wedge^2(V)$ it is $\left[\frac{n+1}{2}\right]$.

Our main aim in this section is to prove that any affine algebraic group is linear, i.e., it is a closed subgroup of GL_n for some n. The proof depends on group actions on algebraic varieties. We will be dealing exclusively with affine algebraic varieties. The coordinate ring of an affine algebraic group G is denoted by $k[G]$, which is same as the space of regular functions on G.

Note that $k[G\times X]\cong k[G]\otimes k[X]$, i.e., polynomial functions on the product space $G\times X$ are a finite linear combination of functions of the form $p(g)q(x)$ where p is a polynomial function on G and q is a polynomial function on X. This crucial property about polynomials goes wrong for almost any other kind of functions.

Exercise 2. Show that $\cos(xy)$ cannot be written as a finite linear combination of functions in x and y alone.

Answer. If $\cos(xy)$ were a finite sum:

$$\cos(xy)=\sum f_i(x)g_i(y),$$

it follows by specialising the y value, that $\cos(ax)$ is a linear combination of finitely many functions $f_i(x)$ for all a, i.e., the space of functions $\cos(ax)$ generates a finite dimensional vector space. But this is false, as for any n, given distinct $a_1,\ldots,a_n\geq 0,\cos(a_ix)$ are linearly independent (Hint: Van der monde determinant).

Proposition. *If X is an affine algebraic variety on which G operates, then any finite dimensional space of functions on X is contained in a finite dimensional space of functions which is invariant under G.*

Proof. It suffices to prove that the translates of a single function is finite dimensional.

Consider $\phi:G\times X\longrightarrow X$. This map gives rise to a ring homomorphism $\phi^*:k[X]\longrightarrow k[G\times X]=k[G]\otimes k[X]$, given by, $f\overset{\phi^*}{\longmapsto}\sum_i\phi_i\otimes f_i$,

i.e., $f(gx)=\sum_i\phi_i(g)f_i(x)$,

i.e., $f^g=\sum_i\phi_i(g)f_i$ and hence $f^g\in$ span of f_i $\forall\, g\in G$. □

Proposition. *If X is affine algebraic variety on which G acts, then a subspace F of $k[X]$ is G-invariant if and only if $\phi^*(F)\subseteq k[G]\otimes F$, where ϕ^* is as in previous proposition.*

Proof. If $\phi^*(F)\subseteq k[G]\otimes F$, then there are functions ϕ_i on $k[G]$ such that $f^g(x)=\sum_i\phi_i(g)f_i(x)$ for $f_i\in F$. So, $f^g\in F$, i.e., F is G-invariant.

To prove the converse, suppose F is G-invariant and let $\{f_r\}$ be a basis of F. We extend this basis to a basis of $k[X]$ by adjoining say $\{g_s\}$. Let $f \in F$. Then, $\phi^*(f) \in k[G] \otimes k[X]$. This implies that $\phi^*(f) = \sum_r a_r \otimes f_r + \sum_s b_s \otimes g_s$, for certain polynomial functions $\{a_r\}, \{b_s\}$ on G. Therefore $f(gx) = \sum_r a_r(g) f_r(x) + \sum_s b_s(g) g_s(x)$. But since F is G-invariant, all b_s are identically zero and hence $\phi^*(F) \subseteq k[G] \otimes F$. □

Theorem. *Any affine algebraic group is linear, i.e., it is isomorphic to a closed subgroup of GL_n for some n.*

Proof. The coordinate ring of G, $k[G]$ is a finitely generated k-algebra, i.e., there exist functions $f_1, \ldots, f_r$ which generate $k[G]$ as an algebra over k. By proposition, one can assume that the subspace generated by f_i's is G-invariant (G acts by left translation).

Thus, $f_i(gx) = \sum m_{ij}(g) f_j(x) \ \forall\, x \in G$, i.e., $f_i^g = \sum m_{ij}(g) f_j$

As $\phi^*(F) \subseteq k[G] \otimes F$, so m_{ij} can be assumed to be algebraic functions on G. This gives rise to a map $\psi : G \longrightarrow GL_n(k)$, given by $g \longmapsto (m_{ij}(g))$, which is a homomorphism of algebraic groups. We will show that this identifies G as a closed subgroup of GL_n. Since the image of an arbitrary map of algebraic groups is closed, the image of G, call it H, is a closed subgroup of GL_n.

We will prove that the surjective mapping $\psi : G \longrightarrow H$ is an isomorphism of algebraic groups. For this, it suffices to prove that the induced map on the coordinate rings $\psi^* : k[H] \longrightarrow k[G]$ is a surjection. But this follows since f_i are in the image of $k[H]$.

This completes the proof. □

Remark. Note that a bijective map need not be an isomorphism of algebraic varieties, as the example $x \longmapsto x^p$ on $\mathbb{A}^1$ in characteristic p shows. As another example, consider the map from $\mathbb{A}^1$ to $\mathbb{A}^2$ given by $x \longmapsto (x^2, x^3)$. This gives a set-theoretic isomorphism of $\mathbb{A}^1$ into the subvariety $\{X^3 = Y^2\} \subseteq \mathbb{A}^2$, but it is not an isomorphism of algebraic varieties. (Why?)

A morphism $f : X \longrightarrow Y$ is called dominant if $f(X)$ is dense in Y; Example: the map $f : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ defined by, $(g_1, g_2) \longmapsto (g_1, g_1 g_2)$.

It can be seen that f is dominant if and only if $f^* : k[Y] \longrightarrow k[X]$ is injective.

It can be seen that f is an isomorphism if and only if f^* is so.

Exercise 3. Classify continuous functions $f : \mathbb{R} \longrightarrow \mathbb{C}$ such that the span of translates of f is finite dimensional.

Answer. It is easy to see that the functions f on $\mathbb{R}$ such that the span of translates of f is finite dimensional is an algebra, i.e., the set of such functions is closed under addition and multiplication. Any polynomial has this property and so do the functions $e^{\lambda x}$. We shall prove that polynomials and exponential functions generate the space of such functions as an algebra.

Let f be a continuous complex valued function on $\mathbb{R}$, and let V be the finite dimensional space spanned by the translates of f. If $\{f_1, \ldots, f_n\}$ is a basis of V, then

$$\phi(t)(f_i)(x) = f_i(t+x) = \sum g_{ij}(t) f_j(x) \ \forall\, t, x.$$

Then $t \longmapsto g_{ij}(t)$ is a matrix coefficient of the finite dimensional representation V of $\mathbb{R}$.

Putting $x = 0$, we get

$$f_i(t) = \sum g_{ij}(t) f_j(0).$$

So f_i are sum of matrix coefficients. Thus, it suffices to understand matrix coefficients of finite dimensional representations. So, we come upon a question, that of classifying finite dimensional continuous representations of $\mathbb{R}$.

Claim. Any finite dimensional representation of $\mathbb{R}$ is of the form $t \longmapsto e^{tA}$ for some matrix $A \in M_n(\mathbb{C})$.

If the representation was analytic, then this follows from Lie algebra methods. However any continuous representation is analytic. We also give another way to characterise finite dimensional representations of $\mathbb{R}$

We write $g(t) = \log(f(t))$ in a neighbourhood of 0. Then, g is a map from $\mathbb{R}$ to $M_n(\mathbb{C})$ such that $t_1 + t_2 \longmapsto g(t_1) + g(t_2)$. As any continuous homomorphism from $\mathbb{R}$ to itself is a scalar multiplication, $g(t) = tA$ for some matrix A. Then $f(t) = exp(tA)$ in a neighbourhood of identity and a neighbourhood of identity generates all of $\mathbb{R}$, so the claim is proved.

Then by canonical form of A,

$$e^{tA} = \sum e^{t\lambda_i}\ exp(tN_i)$$

and $exp(tN_i)$ is a polynomial in t, as N_i are nilpotent. This answers the question.

4. Some Generalities about Closures in the Zariski Topology.

Given $A \subseteq X$, where X is an algebraic variety, one can define $\overline{A}$ to be the smallest closed algebraic subvariety of X containing A, i.e.,

$$\overline{A} \;=\; \bigcap \,\{Y : A \subseteq Y, Y \text{ is closed in } X\}.$$

In particular, if G an algebraic group and H is an abstract subgroup of G, one can talk about $\overline{H}$ which is a closed subvariety of G.

Lemma. *If H is an abstract subgroup of G, then $\overline{H}$ is a closed algebraic subgroup of G.*

Proof. We need to prove $\overline{H} \cdot \overline{H} \subseteq \overline{H}$ and $\overline{H}^{-1} \subseteq \overline{H}$.

Clearly, $H \subseteq h^{-1} \cdot \overline{H}$ for any $h \in H$ and $h^{-1} \cdot \overline{H}$ is also closed in G.

Hence, $\overline{H} \subset h^{-1} \cdot \overline{H}$

$$\begin{aligned}
\Rightarrow \quad & h \cdot \overline{H} \subseteq \overline{H} \quad \forall\, h \in H \\
\Rightarrow \quad & H \cdot \overline{H} \subseteq \overline{H} \\
\Rightarrow \quad & H \cdot \overline{h} \subset \overline{H} \quad \forall\, \overline{h} \in \overline{H} \\
\Rightarrow \quad & \overline{H} \cdot \overline{h} \subset \overline{H} \quad \forall\, \overline{h} \in \overline{H} \\
\Rightarrow \quad & \overline{H} \cdot \overline{H} \subset \overline{H}.
\end{aligned}$$

Similarly by noting that $x \longmapsto x^{-1}$ is a homeomorphism of G, one can prove that $\overline{H}$ is closed under inversion. Thus $\overline{H}$ is a closed subgroup of the algebraic group G. □

This group $\overline{H}$ is called the *algebraic hull* of H.

Proposition. *If $G \subseteq GL_n(\mathbb{C})$ is a subgroup such that for some $e \geq 1$, $x^e = 1 \;\forall\, x \in G$, then G is finite.*

Proof. If G is not finite, look at $\overline{G}$, an algebraic subgroup of $GL_n(\mathbb{C})$, for which $x^e = 1$ continues to hold good. There exists a subgroup of $\overline{G}$ of finite index, G°, such that G° is connected. For a connected algebraic subgroup G°, $G^\circ(\mathbb{C})$ is a Lie group of positive dimension, and then x^e can not be identically 1. Contradiction! □

Let $H \subseteq GL_n(\mathbb{C})$. Thinking of $GL_n(\mathbb{C})$ as an algebraic group defined over $\mathbb{Q}$, one can talk about closure of H as a subgroup of GL_n in the Zariski topology over $\mathbb{C}$ or the one over $\mathbb{Q}$. We have

$$\overline{H} = \bigcap \,\{Y : H \subseteq Y, Y \text{ is closed}\}.$$

If we take only those Y, which are defined over $\mathbb{Q}$, we get the closure of H over $\mathbb{Q}$, which we denote by $\overline{H}^{\mathbb{Q}}$. Clearly $\overline{H}^{\mathbb{Q}} \supseteq \overline{H}$.

Example: Since e is transcendental over $\mathbb{Q}$, the only polynomial $f \in \mathbb{Q}[x]$ with $f(e) = 0$ is the zero polynomial. Hence $\overline{e}^{\mathbb{Q}} = \mathbb{C}$.

Exercise 4. Let G be an algebraic group. Then $\overline{< g >}$ is Abelian. However, if $G = SL_n(\mathbb{C})$, there are elements whose Zariski closure in $\mathbb{Q}$-topology is $SL_n(\mathbb{C})$, so non-Abelian.

Answer.

Mumford-Tate group.

For a smooth Abelian variety X, $H^1(X)$ with coefficients in $\mathbb{Q}$, admits a decomposition over $\mathbb{C}$, called as *Hodge decomposition* as,

$$H^1(X) \otimes_{\mathbb{Q}} \mathbb{C} = H^{0,1} \oplus H^{1,0}.$$

One defines a subgroup of $GL(H^1)$ which is Zariski closure in the $\mathbb{Q}$-topology of the subgroup

$$\left\{ \begin{bmatrix} z & & & & & \\ & \ddots & & & & \\ & & z & & & \\ & & & \overline{z} & & \\ & & & & \ddots & \\ & & & & & \overline{z} \end{bmatrix} : z \in \mathbb{C}^* \right\}.$$

This subgroup is called as the Mumford-Tate group associated to X.

Examples:

(i) If X is a CM elliptic curve, then $MT(X) = k^*$.

(ii) If X is a non-CM elliptic curve, then $MT(X) = GL_2$.

(iii) If X is a Klein curve, then $MT(X) = k^* \times k^* \times k^*$.

Tannaka's Theorem. *A closed subgroup of $SO(n, \mathbb{R})$ (in the Euclidean topology of $\mathbb{R}$) is the set of real points of an algebraic group defined over $\mathbb{R}$.*

Proof. Let G be a closed subgroup of $SO(n, \mathbb{R})$. Any polynomial over $\mathbb{C}$ can be written as $f = f_1 + if_2$ where f_i are polynomials defined over $\mathbb{R}$, then

$$f(z) = 0 \quad \text{if and only if} \quad f_1(z) = 0 \text{ and } f_2(z) = 0.$$

for $z \in SO(n, \mathbb{R})$, therefore $\overline{G}^{\mathbb{C}} = \overline{G}^{\mathbb{R}}$.

We want to prove that $G = \overline{G}(\mathbb{R})$. G is a closed subgroup of $\overline{G}(\mathbb{R})$ which is a closed subgroup of $GL_n(\mathbb{R})$.

Suppose $G \subsetneq \overline{G}(\mathbb{R})$. Let g belong to $\overline{G}(\mathbb{R})$ but not to G. Since $g \in \overline{G}(\mathbb{R})$, every polynomial vanishing on G also vanishes on g. If we can show the existence of a polynomial vanishing on G but not on g, we will be done.

Look at disjoint closed sets G and gG in $\overline{G}(\mathbb{R})$. By Urysohn's lemma, there exists a continuous function f on $\overline{G}(\mathbb{R})$ which is 0 on G and 1 on gG. Observe that the coordinate functions $\{m_{ij}(g)\}$ are continuous functions on G, and hence by Stone-Weierstrass theorem, the algebra generated by m_{ij} is dense in $\mathbb{C}(\overline{G}(\mathbb{R}))$. Therefore, there exists a polynomial in m_{ij}, say $p(m_{ij})$, which approximates f very closely on $\overline{G}(\mathbb{R})$.

But this polynomial need not be identically zero on G which is what we want to achieve. To this end, we define

$$F(\overline{g}) \;=\; \int_G p(m_{ij})(\overline{g}h)dh.$$

Since F is a right G-invariant function, it is constant on G and on gG. Thus $F = \epsilon_1$ on G and $F = \epsilon_2$ on gG, where we can assume that ϵ_1 is very close to 0, and ϵ_2 is very close to 1. Then by suitable translation, F is 0 on G and nonzero at g. So, the only remaining thing to prove is that F is a polynomial again in m_{ij}.

We note the property of matrix coefficients that

$$m_{ij}(gh) = \sum_k m_{ik}(g) \cdot m_{kj}(h).$$

Therefore for any polynomial p in the n^2-variables m_{ij}, we have

$$p(m_{ij})(gh) = \sum_{P,Q} P(m_{ij})(g)Q(m_{ij})(h)$$

where P and Q are certain polynomials in m_{ij}.

This completes the proof. □

Exercise 5. If V is a faithful representation of a compact group G, then any irreducible representation W is contained in $V^{\otimes r} \otimes V^{*\otimes s}$.

Answer. Assume the contrary, then

$$\int g^W f^V = 0$$

for all matrix coefficients g^W of W and f^V of $V^{\otimes r} \otimes V^{*\otimes s}$. The $\mathbb{C}$-sum of matrix coefficients of $V^{\otimes r} \otimes V^{*\otimes s}$ forms a subalgebra of functions on G. So

$$\int g^W f = 0$$

for all g^W and all f in this subalgebra. But by Stone-Weierstrass theorem, this subalgebra is dense on G. Contradiction!

Corollary.

(i) *If V is any faithful representation, then the algebra generated by the matrix coefficients of V is independent of V.*

(ii) (Coro. of Exer. 3 and Exer. 5) *The space of functions f in $\mathbb{C}[G]$ which span a finite dimensional space under left (right) translations is precisely the algebra of matrix coefficients of finite dimensional representations.*

For a compact group $G \hookrightarrow SO(n, \mathbb{R})$, we discussed about algebraic closure of G, viz. G^{alg} in $\mathbb{R}$-Zariski topology such that $G^{alg}(\mathbb{R}) = G$. G^{alg} is called the complexification of G, in the sense that $Lie(G) \otimes \mathbb{C} = Lie(G^{alg})(\mathbb{C})$.

The above statement need not be true for non-compact groups. Torus creates some problems. The torus $\mathbb{R}^* \times \mathbb{R}^*$ has few algebraic characters, but many topological characters.

Peter-Weyl Theorem.

(i) *Any compact Lie group has a faithful representation.*

(ii) $L^2(G) \cong \sum_V V \otimes V^*$ *as $G \times G$ module, where V runs over all irreducible representations of G.*

5. Lie Algebras associated to Algebraic Groups.

Let k be a ring, A a commutative k-algebra and M an A-module. A *derivation* d of A with values in M is a map $d : A \longrightarrow M$, such that

$$d(a+b) = d(a) + d(b) \ \forall\, a, b \in A$$

$$d(ab) = ad(b) + bd(a) \ \forall\, a, b \in A$$

$$d(\lambda a) = \lambda d(a) \ \forall\, \lambda \in k, a \in A.$$

(Observe that $d(r) = 0 \ \forall\, r \in k$.) The space of derivations of A with values in an A-module M is naturally an A-module. If $M = A$, then a derivation of A with values in M is called a derivation on A.

Examples:

(i) $A = k[x] = M$, then any derivative is of the form $d(g) = f(x)\frac{d}{dx}(g)$, for some $f \in k[x]$. Hence, the space of derivations is free of rank 1 over $A = k[x]$.

(ii) $A = k[x_1, \ldots, x_n] = M$, the derivations $\frac{\partial}{\partial x_i}$ form a free basis of the space of derivations over A.

Exercise 6. Justify above statement.

Answer. Let d be a derivation. Define $d(x_i) = f_i$. Now, we have two derivations $d_1 = \sum f_i \frac{\partial}{\partial x_i}$ and d, but they are same on generators, viz., x_i, so they are same on the full algebra $k[x_1, \ldots, x_n]$.

Corollary. *The space of derivations on $A = k[x_1, \ldots, x_n]$ is a free A-module of rank equal to the dimension of A over k.*

Let $O_{X,x}$ be the ring of germs of functions at a point $x \in X$, where X is either a manifold or an algebraic variety over a field k.

In algebraic geometry, $O_{X,x}$ is the space of rational functions $\frac{f}{g}$, where f and g are polynomial functions defined in a neighbourhood of the point x and $g(x) \neq 0$, whereas in topology $O_{X,x}$ is the space of C^∞ functions defined in a neighbourhood of x.

$A = O_{X,x}$, $M = k = O_{X,x}/\mathfrak{m}_x$, where $\mathfrak{m}_x := \ker\{f \longmapsto f(x)\}$. A derivation in this case is called a *tangent vector* at $x \in X$.

Let $T : O_{X,x} \longrightarrow k$ be a derivation, i.e., T has the property that $T(fg) = f(x)T(g) + g(x)T(f)$. Then $T(1) = T(1) + T(1)$. Therefore $T(1) = 0$. Also $T : \mathfrak{m}_x \longrightarrow k$ factors through ${\mathfrak{m}_x}^2$, so it induces a map : $\mathfrak{m}_x/{\mathfrak{m}_x}^2 \longrightarrow k$. We will prove that the tangent vectors at $x \in X$ can be canonically identified to $(\mathfrak{m}_x/{\mathfrak{m}_x}^2)^*$. The space of tangent vectors at $x \in X$ is denoted by $T_{X,x}$.

Note that $\mathfrak{m}_x/\mathfrak{m}_x{}^2$ is a finite dimensional k-vector space (follows from Noetherianness and Nakayama's lemma). We have the inequality

$$\dim\left(\mathfrak{m}_x/\mathfrak{m}_x{}^2\right) \geq \dim X \;\; \forall\, x \in X.$$

When equality holds, we say x is a smooth point.

In characteristic 0, the set of singular points is a proper closed subvariety. In any characteristic, the Jacobian criterion is satisfied.

Jacobian Criterion. *If $f(x_1, \ldots, x_n) = 0$ the is equation of a variety, then x is smooth if and only if there exists i such that $\frac{\partial f}{\partial x_i} \neq 0$ at x.*

A derivation $d = \sum f_i \frac{\partial}{\partial x_i}$ is visualised as associating vectors $(f_1(x), \ldots, f_n(x))$ to any point x.

Lemma.

(i) $T_{X,x} \cong \operatorname{Hom}_k\left(\mathfrak{m}_x/\mathfrak{m}_x{}^2, k\right)$.

(ii) *When $k = \mathbb{R}$, for any point x on an n-dimensional $\mathbb{R}$-manifold X, $\mathfrak{m}_x/\mathfrak{m}_x{}^2$ is an n-dimensional $\mathbb{R}$-vector space.*

Proof. (i) Observe that $d(\mathfrak{m}_x{}^2) = 0$, as $d(fg) = f(x)dg + g(x)df$ and $f, g \in \mathfrak{m}_x$ therefore $f(x) = g(x) = 0$. So d factors through $\mathfrak{m}_x{}^2$, hence $d \in \operatorname{Hom}_k\left(\mathfrak{m}_x/\mathfrak{m}_x{}^2, k\right)$.

Conversely, we need to prove that a k-linear map $T : \mathfrak{m}_x/\mathfrak{m}_x{}^2 \longrightarrow k$ gives rise to a derivation.

We define $d(f) = T(f - f(x))$. Clearly d is linear. Now, $d(fg) = T(fg - fg(x))$ and $fdg + gdf = fT(g - g(x)) + gT(f - f(x))$. Hence to prove $d(fg) = f(x)dg + g(x)df$, we need to prove

$$T(fg - f(x)g(x) - f(x)g + f(x)g(x) - g(x)f + f(x)g(x)) = 0.$$

This follows as

$$fg - f(x)g - g(x)f + f(x)g(x) = \big(f - f(x)\big)\big(g - g(x)\big) \in \mathfrak{m}_x{}^2.$$

For (ii), we have $\dim\left(\mathfrak{m}_x/\mathfrak{m}_x{}^2\right) \geq n$ as $\frac{\partial}{\partial x_i}$ are linearly independent over $\mathbb{R}$. To prove other inequality we use following fact.

Any $f \in C^\infty(\mathbb{R}^n)$ can be written locally around the origin as

$$f = f(0) + \sum f_i X_i + \sum g_{ij} X_i X_j$$

where f_i are constants and $g_{ij} \in C^\infty(\mathbb{R}^n)$. □

Thus $T_{X,x}$, the space of derivations on $O_{X,x}$, is an n-dimensional vector space, called the *tangent space to X at x*. A typical element of $T_{X,x}$ looks like $\sum f_i \frac{\partial}{\partial x_i}$, where f_i are some constants.

A map, $x \longmapsto v_x \in T_{X,x}$, varying smoothly, is called a *vector field*, i.e., if we write $v_x = \sum f_i(x) \frac{\partial}{\partial x_i}$, then f_i are smooth functions.

One can also define smoothness of a vector field V by saying that $V(f)$ is a smooth function for all f smooth.

Given vector fields V_1 and V_2, one defines another vector field $[V_1, V_2] = V_1 V_2 - V_2 V_1$. More precisely

$$[V_1, V_2](f) = V_{1,x}(V_2 f) - V_{2,x}(V_1 f).$$

This can be checked to be a vector field, called the *Lie bracket*. This defines a Lie algebra structure on the set of vector fields on a manifold.

Functorial Properties of tangent spaces. If $f : X \longrightarrow Y$ is a morphism, then we have a map $df : T_{X,x} \longrightarrow T_{Y,f(x)}$ given by, $df(v)(\phi) = v(\phi \circ f)$.

Caution: One cannot use df to push vector fields from X to Y as there might be several points in X with the same image in Y.

If V_1 is a vector field on X and V_2 on Y, then V_2 is f-related to V_1 if, for all $x \in X$, $(df)_x : T_{X,x} \longrightarrow T_{Y,f(x)}$ sends $V_{1,x}$ to $V_{2,f(x)}$.

In particular, if G is a group which operates on a manifold X in a differentiable way, it makes sense to talk about vector fields on X, invariant under G.

Examples:

(i) On $\mathbb{R}$, any vector field d looks like $f(x)\frac{d}{dx}$. The group $\mathbb{R}$ acts on itself by translations and only vector field invariant under addition is $\lambda \frac{d}{dx}$ for λ a constant.

(ii) On $\mathbb{R}^*$, $x\frac{d}{dx}$ is the only invariant vector field upto scalar multiple.

(iii) Consider the group $GL_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$. A vector field on $GL_n(\mathbb{R})$ looks like $\sum a_{ij}(X)\frac{\partial}{\partial X_{ij}}$. Any left-invariant vector field corresponds to a matrix $(b_{ij}) \in M_n(\mathbb{R})$, and the invariant vector field is $\sum_{i,j,k} b_{ik}X_{kj}\frac{\partial}{\partial X_{ji}}$.

Exercise 7. Justify above sentence. (Hint: Change of variables)

Proposition. *If $0 \in X \subseteq k^n$, where X is defined by polynomial equations $f_i(x_1, \ldots, x_n) = 0$, then the tangent space to X at 0 is defined by degree 1 part of f_i.*

Proof. As $0 \in X, f_i(0, \ldots, 0) = 0$. We write $f_i(x_1, \ldots, x_n) = \sum b_\lambda x_\lambda + \ldots$. We have already noted that $T_{X,x} \cong (\mathfrak{m}_x/\mathfrak{m}_x{}^2)^*$. We note that if X is a closed subvariety of $\mathbb{A}^n$, then the ring of polynomial functions on X, i.e., $k[X]$ is a quotient of $k[x_1, \ldots, x_n]$, hence derivations of $k[X]$ at any point of X can be identified to a subspace of the space $\{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\}$. Hence

$$\frac{\mathfrak{m}_0}{\mathfrak{m}_0^2} \cong \frac{< x_1, \ldots, x_n >}{I+ < x_1, \ldots, x_n >^2}.$$

Examples: 1. The curve $X^2 = Y^3$ at $(0,0)$ has 2-dimensional tangent space at $(0,0)$ as there is no linear term. Similarly the tangent space to the curve $X^2 = Y^2$ is 2-dimensional.

2. $X = Y^4 + Z^7$ has 2-dimensional tangent space given by $\frac{\partial}{\partial Y}, \frac{\partial}{\partial Z}$.

One can calculate Lie algebra associated to algebraic groups by using above proposition.

$$O(n) = \{A \in GL_n : {}^tAA = I\} \subseteq M_n.$$

We propose to calculate the tangent space at I. We replace A by $I + X$. Then we have ${}^t(I + X)(I + X) = I$, i.e., ${}^tX + X + {}^tXX = 0$. And then the linear terms ${}^tX + X = 0$ define the tangent space at I.

Another way to look at derivations:

Lemma.

(i) *The ring homomorphisms $\phi : A \longrightarrow \frac{A[\epsilon]}{(\epsilon^2)}$ with $\phi(a) = a + \epsilon\phi_1(a)$ are in bijective correspondence with the set of derivations on A.*

(ii) *Let X be a variety and $A = k[X]$. A ring homomorphism $\phi : A \longrightarrow \frac{k[\epsilon]}{(\epsilon^2)}$ when composed with the natural map from $\frac{k[\epsilon]}{(\epsilon^2)}$ to $k = \frac{k[\epsilon]}{(\epsilon)}$ defines a* *point on the variety X. The set of ring homomorphisms from A to $\frac{k[\epsilon]}{(\epsilon^2)}$ written as $\phi(a) = \phi_0(a) + \epsilon\phi_1(a)$ is in bijective correspondence with the tangent space associated to the point $x \in X$ defined by ϕ_0.*

Proof. (i) If $d : A \longrightarrow A$ is a derivation on A, then one can check that the map $\phi : A \longrightarrow \frac{A[\epsilon]}{\epsilon^2}$ given by, $a \longmapsto a + \epsilon d(a)$ defines a ring homomorphism. Conversely, if $\phi(a) = a + \epsilon\phi_1(a)$ is one such ring homomorphism, then ϕ_1 is a derivation on A.

(ii) Here we note that the map $k[X] \xrightarrow{\phi} \frac{k[\epsilon]}{(\epsilon^2)} \longrightarrow \frac{k[\epsilon]}{(\epsilon)} = k$ is precisely the evaluation at a point $x \in X$. This is precisely the way a point on a variety is defined. Then rest follows as above. □

Proposition. *Suppose there exists a morphism $\phi : G \times X \longrightarrow X$ of affine algebraic varieties. Then there exists a map ψ from $T_e(G)$ to the set of vector fields on X. If A is an automorphism of X which commutes with the action of G, i.e., $g(Ax) = A(gx)$, then $\psi(v)$ is an invariant vector field on X. Moreover there exists a map from $T_e(G) \oplus T_x(X)$ to $T_x(X)$.*

Proof. We have $\phi : G \times X \longrightarrow X$. This gives rise to a map on the level of coordinate rings, $\phi^* : k[X] \longrightarrow k[G] \otimes k[X]$. Let $v \in T_e(G)$. By second part in the previous lemma, we get a ring homomorphism $\phi_v : k[G] \longrightarrow \frac{k[\epsilon]}{(\epsilon^2)}$. The ring homomorphism ϕ^* when composed with ϕ_v, gives rise to a vector field on X as shown in the commutative diagram below. We define it to be $\psi(v)$. Thus we get a map ψ from $T_e(G)$ to the set of vector fields on X.

$$\begin{tikzcd}
k[X] \arrow[r, "\phi^*"] \arrow[dr, dashed, "\psi(v)"'] & k[G] \otimes k[X] \arrow[d, "\phi_v"] \\
 & \frac{k[\epsilon]}{(\epsilon^2)} \otimes k[X] = \frac{k[X][\epsilon]}{(\epsilon^2)} \ .
\end{tikzcd}$$

Now, if A be an automorphism of X which commutes with the G-action, then we have following commutative diagram:

$$\begin{tikzcd}
G \times X \arrow[r, "\phi"] \arrow[d, "\mathrm{Id}\times A"'] & X \arrow[d, "A"] \\
G \times X \arrow[r, "\phi"] & X
\end{tikzcd}$$

This gives us another commutative diagram:

$$\begin{tikzcd}
k[X] \arrow[r, "\phi^*"] \arrow[d, "A^*"'] & k[G] \otimes k[X] \arrow[r, "\phi_v"] \arrow[d, "\mathrm{Id} \otimes A^*"'] & \frac{k[X][\epsilon]}{(\epsilon^2)} \arrow[d, "B^*"] \\
k[X] \arrow[r, "\phi^*"] & k[G] \otimes k[X] \arrow[r, "\phi_v"] & \frac{k[X][\epsilon]}{(\epsilon^2)}\ ,
\end{tikzcd}$$

where B^* is the natural extension of A^* to $\frac{k[X][\epsilon]}{(\epsilon^2)}$. Thus we get a vector field, which commutes with every G-invariant automorphism of X. Now, consider $X = G$ and consider the left action of G on itself, then to every tangent vector at e to G, we get a vector field on G which is right invariant. Similarly $T_e(G)$ could be identified to left invariant vector fields. The vector field X_v associated to a vector $v \in T_e(G)$ has $X_v(e) = v$.

Now, we want to give a map from $T_e(G) \oplus T_x(X) \longrightarrow T_x(X)$. For a $v \in T_e(G)$, we have a vector field $\psi(v) : k[X] \longrightarrow \frac{k[X][\epsilon_1]}{(\epsilon_1^2)}$. Consider the map given by

$$k[G] \otimes k[X] \longrightarrow \frac{k[\epsilon_1]}{(\epsilon_1^2)} \otimes \frac{k[\epsilon_2]}{(\epsilon_2^2)} \xrightarrow{\phi_{\lambda,\mu}} \frac{k[\epsilon]}{(\epsilon^2)}$$

where the ring homomorphisms $\phi_{\lambda,\mu}$ are parametrised by the maps $\epsilon_1 \mapsto \lambda\epsilon$ and $\epsilon_2 \mapsto \mu\epsilon$. So, we have

$$\begin{tikzcd}
k[X] \arrow[r] \arrow[rrd, dashed] & k[G] \otimes k[X] \arrow[r] & \frac{k[\epsilon_1]}{(\epsilon_1^2)} \otimes \frac{k[\epsilon_2]}{(\epsilon_2^2)} \arrow[d, "\begin{matrix} \epsilon_1 \mapsto \epsilon \\ \epsilon_2 \mapsto \epsilon \end{matrix}"] \\
 & & \frac{k[\epsilon]}{\epsilon^2}
\end{tikzcd}$$

$\square$

Corollary. *The space $T_e(G)$ is isomorphic to the space of left G-invariant vector fields on G.*

Thus $T_e(G)$ acquires a Lie algebra structure.

Theorem. (Lie algebra of a Lie group). *If G is a Lie group, then the set of left invariant vector fields forms a finite dimensional vector space $\mathfrak{g}$ which is closed under Lie brackets; and is called the Lie algebra associated to the Lie group G. Moreover, $\dim \mathfrak{g} = \dim G$.*

Proof. Follows from previous proposition and its corollary. □

6. More about Algebraic Groups.

In the next two sections, we shall sketch an outline of the theory of affine algebraic groups. We shall avoid proving theorems. Our emphasis will be on exposition. We mainly follow Springer's book for the exposition. We also list some open questions in this area.

We have already noted that an affine algebraic group is a closed subgroup of GL_n for some n. We also know that every matrix $g \in GL_n$ admits a decomposition, called as Jordan decomposition, as $g = g_s g_u$, where g_s is semi-simple (i.e., g_s is diagonalisable over $\overline{k}$) and g_u is unipotent (i.e., every eigenvalue of g_u is 1). Moreover $g_s g_u = g_u g_s$. If $g \in G \hookrightarrow GL_n$, then $g_s, g_u \in G$. This decomposition is called as the *Jordan decomposition* in the algebraic group G. More generally, if $\phi : G \longrightarrow G'$ is a homomorphism of algebraic groups then $\phi(g)_s = \phi(g_s)$ and $\phi(g)_u = \phi(g_u)$. An element $g \in G$ is said to be *unipotent* if $g = g_u$.

A *unipotent algebraic group* is the one in which every element is unipotent. Example: The simplest unipotent group is $\mathbb{G}_a$, given by

$$\mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in k \right\}.$$

Theorem. *Unipotent algebraic groups are precisely the closed subgroups of upper unitriangular group U_n, (upto conjugacy), for some n.*

A consequence of the above theorem is that for a representation of a unipotent algebraic group G in GL_n, there is a non-zero vector in k^n fixed by all of G. And using this fact, we get the following

Proposition. *Let X be an affine variety admitting an action of a unipotent algebraic group G, then all orbits of G in X are closed.*

Classification of unipotent algebraic groups is not well understood. The unipotent algebraic groups can vary in continuous families, i.e., there exists $U(s)$ unipotent algebraic group parametrised by a complex number s such that for $s_1 \neq s_2$, $U(s_1) \ncong U(s_2)$.

A *solvable* (resp. *nilpotent*) *algebraic group* is an algebraic group which is solvable (resp. nilpotent) as an abstract group. If H and K are subgroups of an algebraic group G, $[H, K]$ denotes the closed subgroup of G generated by the set $\{xyx^{-1}y^{-1} : x \in H, y \in K\}$.

A unipotent group is a closed subgroup of U_n, and hence is solvable (in fact, it is nilpotent). More precisely, for a unipotent group U, we define $U^1 = U$ and $U^i = [U, U^{i-1}]$. Then U^i/U^{i+1} is an Abelian group, isomorphic to $\mathbb{G}_a^{d(i)}$ for some integer $d(i)$.

Question. *Is the set of unipotent groups, with given integers $d(i)$, a connected family? Is it an algebraic variety?*

Examples in Riemann surfaces suggest that this family is not an algebraic variety, but a quotient of a variety. More concretely, one could ask following

Question. *Classify integers $d(i)$ such that this family is positive dimensional.*

The theory of unipotent algebraic groups is also closely connected with classification of p-groups which is yet an unsolved (unsolvable?) problem.

The subgroup $U_n(\mathbb{F}_p)$ of $GL_n(\mathbb{F}_p)$ consisting of all upper triangular unipotent matrices is a Sylow-p subgroup of $GL_n(\mathbb{F}_p)$. Therefore, just like unipotent algebraic groups, every p-subgroup of $GL_n(\mathbb{F}_p)$ is also a subgroup of upper triangular unipotent matrices, upto conjugacy.

Exercise 8. Prove that for $n < p$, there exists a bijective correspondence between subgroups of $U_n(\mathbb{F}_p)$ and connected algebraic subgroups of U_n defined over $\mathbb{F}_p$.

(Hint: Associating a Lie algebra to an abstract unipotent group.)

Question. *$H^*(U_n(\mathbb{F}_p), \mathbb{F}_p)$ is an algebra over $\mathbb{F}_p$. Construct this algebra out of information coming from $H^*(\mathfrak{u}_n, \mathbb{C})$, where $\mathfrak{u}_n$ is the Lie algebra of upper triangular unipotent matrices.*

Theorem. (Lie-Kolchin). *A connected solvable algebraic group is a subgroup of upper triangular matrices (upto conjugacy).*

Corollary. *If G is a connected solvable algebraic group, then $[G, G]$ is nilpotent.*

Proposition. *Let G be a connected nilpotent algebraic group.*

(i) *The sets G_s, G_u of semi-simple and unipotent elements (resp.) are closed, connected subgroups of G and G_s is a central torus of G.*

(ii) *The product map $G_s \times G_u \longrightarrow G$ is an isomorphism of algebraic groups.*

Proposition. *For a connected solvable group G, the commutator subgroup $[G,G]$ is a closed, connected, unipotent, normal subgroup. The set G_u of unipotent elements is a closed, connected, nilpotent, normal subgroup of G. The quotient group G/G_u is a torus.*

In other words, for a solvable group G, there exists an exact sequence

$$0 \longrightarrow G_u \longrightarrow G \longrightarrow \mathbb{G}_m^r \longrightarrow 1.$$

In fact, this sequence is split, and the reason is the Jordan decomposition!

Another important class of algebraic groups is that of commutative algebraic groups. A commutative algebraic group is solvable, so all above results of solvable groups hold for connected commutative groups as well.

Lemma. *A connected linear algebraic group G of dimension one is commutative and it is isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$.*

A linear algebraic group G is said to be *diagonalisable* if it is a closed subgroup of D_n, the group of diagonal matrices in GL_n, for some n.

Lemma. *An algebraic group G is diagonalisable if and only if any representation of G is a direct sum of one dimensional representations.*

Theorem. *Let G be a diagonalisable group. Then*

(i) *G is a direct product of a torus and a finite Abelian group of order prime to p, where p is the characteristic of k;*

(ii) *G is a torus if and only if it is connected.*

Rigidity of diagonalisable groups. *Let G and H be diagonalisable groups and let V be a connected affine variety. Let $\phi : V \times G \longrightarrow H$ be a morphism such that for any $v \in V$, the map $x \longmapsto \phi(v,x)$ defines a homomorphism of algebraic groups $G \longrightarrow H$. Then $\phi(v,x)$ is independent of v.*

For a subgroup H of an algebraic group G, we define the centraliser and normaliser of H in G as,

$$Z_G(H) := \{g \in G : ghg^{-1} = h \ \forall\, h \in H\};$$

$$N_G(H) := \{g \in G : ghg^{-1} \in H \ \forall\, h \in H\}.$$

Corollary. *If H is a diagonalisable subgroup of G, then $N_G(H)^\circ = Z_G(H)^\circ$ and $N_G(H)/Z_G(H)$ is finite.*

A subgroup $P \hookrightarrow G$ is called *parabolic subgroup* if G/P is a projective variety.

Proposition.

(i) *If H is a parabolic subgroup of G and K is a closed subgroup, then $H \cap K$ is a parabolic subgroup of K.*

(ii) *If H is a parabolic subgroup of K and K is a parabolic subgroup of G, then H is a parabolic subgroup of G.*

(iii) *Any closed subgroup of G containing a parabolic subgroup is itself parabolic.*

(iv) *H is a parabolic subgroup of G if and only if H° is parabolic in G°.*

Borel's fixed point theorem. *If G is a connected solvable group operating on a projective variety X, then G has a fixed point.*

Proof. We prove this result by using induction on $\dim G$. If $\dim G = 0$, $G = (e)$. Now let $\dim G > 0$, then $H = [G, G]$ is a closed, connected subgroup of smaller dimension. Hence by induction hypothesis, the set of fixed points of H in X, say Y, is non-empty and closed in X, thus Y itself is a projective variety. Since H is normal in G, Y is stable under the G-action. We know that for a group action, closed orbits always exist. Let $y \in Y$ such that the orbit Gy is closed in Y. Look at the isotropy subgroup G_y of y in G. Then G_y is closed subgroup of G and as $H \subseteq G_y$, G_y is also normal in G. Hence G/G_y is an affine variety. But then $G/G_y = Gy$, which is projective. Therefore, Gy must be a point, a fixed point of the G-action.

This completes the proof. □

A *Borel subgroup* of G is a maximal connected solvable subgroup of G. Example: If $G = GL_n$, then the subgroup of upper triangular matrices is a Borel subgroup.

A maximal flag in k^n is a strictly increasing sequence of subspaces of k^n, $\{0\} \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = k^n$. Borel subgroups in GL_n correspond bijectively to the set of maximal flags in k^n. The group GL_n operates transitively on the set of maximal flags and isotropy subgroup of the standard flag, $\{0\} \subsetneq \{e_1\} \subsetneq \{e_1, e_2\} \subsetneq \cdots \subsetneq \{e_1, \ldots, e_n\}$ is the Borel subgroup described above, i.e., the subgroup of GL_n consisting of all upper triangular matrices.

Theorem.

(i) *All Borel subgroups are conjugates.*

(ii) *Every Borel subgroup of G is a parabolic subgroup.*

(iii) *A subgroup of G is parabolic if and only if it contains a Borel subgroup.*

(iv) *Every element of G lies in a Borel subgroup. In other words, union of Borel subgroups cover whole of G.*

Proposition. *Let B be a Borel subgroup of an algebraic group G. Then,*

(i) $N(B) = B$.

(ii) $Z(B) = Z(G)$.

(iii) *Any subgroup of G which contains a Borel is always connected.*

7. Structure Theory of Reductive Groups.

Here k is a field, not necessarily algebraically closed.

The *unipotent radical* of an algebraic group G is the maximal normal unipotent subgroup of G.

Such a subgroup always exists. If U_1, U_2 are two normal unipotent subgroups of G, then it can be easily checked that $U_1 \cdot U_2$ is again a normal unipotent subgroup. Then by dimension argument, one must get a maximal subgroup of G with these properties. The unipotent radical of G is denoted by $R_u(G)$. Example: If G is the subgroup of GL_2 consisting of all upper triangular matrices, then $R_u(G)$ is precisely the subgroup of matrices with diagonal entries both equal to 1.

The *radical* of a group G is the maximal connected normal solvable subgroup of G and it is denoted by $R(G)$. One can prove existence of such a subgroup by similar reasoning as above. Also, $R_u(G) = R(G)_u$. Example: If $G = GL_n$, then $R(G)$ is the subgroup of scalar matrices.

An algebraic group $G \hookrightarrow GL_n$ is called *reductive* if $R_u(G)$ is trivial. Example: GL_n.

An algebraic group G is called *simple* if it is non-Abelian and has no connected normal subgroup other than G and (e). Example: SL_n.

An algebraic group G is called *semi-simple* if it is an almost product of simple groups, i.e., $G = G_1 \cdots G_n$, $G_i \cap G_j \subseteq Z(G)$ for $i \neq j$, and all G_i commute with each other. Equivalently, an algebraic group G is called semi-simple if $R(G)$ is trivial. Clearly, every simple algebraic group is semi-simple and every semi-simple algebraic group is reductive.

Theorem. *Any reductive group is upto a center, an almost product of simple groups.*

Theorem. *If $k = \overline{k}$, then there exists bijective correspondence between simple groups over k and compact simple groups over $\mathbb{R}$.*

This bijection is achieved via the root systems.

We recall that a *torus* is a diagonalisable commutative group. A torus $T \hookrightarrow G$ is called a *maximal torus* if it is of maximum possible dimension. Example: The subgroup of diagonal matrices in GL_n is a maximal torus in GL_n.

Theorem. *Any two maximal tori of an algebraic group are conjugates over $\overline{k}$.*

In particular, dimension of a maximal torus in G is a fixed number. We define it to be the *rank* of the group G.

For a maximal torus $T \hookrightarrow G$, we define *Weyl group* of G with respect to T as $N(T)/T$. It is independent of the maximal torus if $k = \overline{k}$, in that case we simply denote it by W. Example: The rank of GL_n is n.

Bruhat Decomposition. *Let G be a reductive group, then for a fixed Borel subgroup B,*

$$G = \coprod_{w \in W} BwB.$$

There is the notion of a BN-pair, where $N = N(T)$, for $T \subseteq B$, a maximal torus. These notions were developed by Tits, based on Chevalley's work, to prove that $G(k)$ is abstractly simple group when G is simple.

Theorem. *Let G be a simple algebraic group defined over k. Suppose that G is split, i.e., G contains a maximal torus which is isomorphic to $\mathbb{G}_m^d$ over k, where d is the rank of G. Then except for a few exceptions $G(k)/Z$ is a simple abstract group.*

The exceptions are $G = SL_2(\mathbb{F}_2)$ and $SL_2(\mathbb{F}_3)$.

There is a notion of quasi-split groups. These are the groups that contain a Borel subgroup defined over k.

Theorem. (Lang). *Any reductive algebraic group over a finite field is quasi-split.*

Steinberg proved analogue of Chevalley's theorem for quasi-split groups.

The group $SO(p,q)$ is quasi-split if and only if $|p-q| \leq 2$.
The group $U(p,q)$ is quasi-split if and only if $|p-q| \leq 1$.

Kneser-Tits Conjecture. *Let G be a simply connected algebraic group. If there exists a map from $\mathbb{G}_m$ to G (i.e., G is isotropic), then $G(k)/Z$ is simple.*

Platonov proved that this conjecture is false in general, but true over global and local fields.

An algebraic group is called as *anisotropic* if it does not contain any subgroup isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. Example: $SO(2n,\mathbb{R})$, another example is $SL_1(D)$, the group of norm 1 elements in a division algebra D.

Question. *Which $SL_1(D)$ are simple?*

Platonov-Margulis Conjecture. *Over a number field k, $SL_1(D)$ is simple if and only if $D \otimes k_v$ is never a division algebra for a non-Archimedean valuation v of k.*

The question of classifying algebraic groups over general fields forms a part of Galois cohomology. This is known only for number fields or their completions.

Theorem. *Let k be either a number field or its completion. The tori over k of dimension n are in bijective correspondence with isomorphism classes of $Gal(\overline{k}/k)$-modules, free over $\mathbb{Z}$ of rank n.*

Example: The tori over $\mathbb{R}$ are the following

$$T \cong (S^1)^{r_1} \times (\mathbb{C}^*)^{r_2} \times (\mathbb{R}^*)^{r_3}.$$

This amounts to classifying matrices of order 2 in $GL_n(\mathbb{Z})$.

$$\{e \longmapsto e\} \longleftrightarrow \mathbb{R}^*$$
$$\{e \longmapsto -e\} \longleftrightarrow S^1$$

$$\begin{Bmatrix} e_1 \longmapsto e_2 \\ e_2 \longmapsto e_1 \end{Bmatrix} \longleftrightarrow \mathbb{C}^*$$

Any invariant in $GL_n(\mathbb{Z})$ is a direct sum of these.

Rationality question. *The question is whether $k[G]$ is unirational/rational for an algebraic group G, i.e., whether $k[G]$ is a purely transcendental extension of k or contained inside one such.*

The answer for above question is yes for groups of type B_n, C_n, D_n.

Cayley Transform: Let $G = SO(n) = \{{}^tAA = I\}$. Let X be a skew symmetric matrix, i.e., ${}^tA + A = 0$. If no eigenvalue of such an X is 1, then $I - X$ is invertible, and it can be checked that $(I+X)(I-X)^{-1}$ belongs to $SO(n)$. This gives a birational map from the Lie algebra of $SO(n)$ to $SO(n)$, proving the rationality of $SO(n)$.

8. Galois Cohomology of Classical Groups

Let G be a group, and A another group on which G acts via group automorphisms: $g(ab) = g(a)g(b)$. Define,

$$A^G = \{a \in A | g \cdot a = a \quad \forall g \in G\} = H^0(G, A).$$

If A is commutative, then $H^i(G, A)$ are defined for all $i \geq 0$, and these are abelian groups.

If A is non-commutative, then 'usually' only $H^1(G, A)$ is defined, and it is a pointed set:

$$H^1(G, A) = \frac{\{\phi : G \to A | \phi(g_1 g_2) = \phi(g_1) \cdot g_1 \phi(g_2)\}}{\{\phi \sim \phi_a \text{ where } \ \phi_a(g) = a^{-1}\phi(g)g(a)\}}.$$

If

$$0 \to A \to B \to C \to 0,$$

is an exact sequence of groups, then there exists a long exact sequence:

$$\begin{aligned} 0 \ &\to \ H^0(G, A) \to H^0(G, B) \to H^0(G, C) \\ &\to \ H^1(G, A) \to H^1(G, B) \to H^1(G, C) \end{aligned}$$

This is a long exact sequence of pointed sets: inverse image of the base point = image of the previous map.

If

$$0 \to A \to B \to C \to 0,$$

is an exact sequence of abelian groups, then

$$\begin{aligned} 0 &\to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \\ &\to H^1(G,A) \to H^1(G,B) \to H^1(G,C) \end{aligned}$$

is a long exact sequence of abelian groups.

Let E be an algebraic group over a field k, for instance the groups like $\mathbb{G}_m, \mathbb{G}_a, GL_n,$

$SO_n, Sp_{2n}, \mu_n, \mathbb{Z}/n$. Then it makes sense to talk of $E(K)$ for K any field extension of k, or in fact any algebra containing k.

If A is a commutative algebraic group over k, one can talk about $H^i(\mathrm{Gal}(K/k), A(K))$ for all finite Galois extensions K of k, whereas if A is noncommutative, we can talk only about the set $H^1(\mathrm{Gal}(K/k), A(K))$.

Define

$$H^i(k,A) = \mathrm{Lim}_K H^i(\mathrm{Gal}(K/k), A(K)),$$

direct limit taken over all finite Galois extensions K of k.

The group/set $H^i(k,A)$ is called the i-th Galois cohomology of A over k.

Example :

1. $H^i(k, \mathbb{G}_a) = 0$ for all $i \geq 1$. This is a consequence of the normal basis theorem.

2. $H^1(k, \mathbb{G}_m) = 0$. This is the so-called Hilbert's theorem 90.

3. $H^1(k, GL_n) = 0$.

4. $H^2(k, \mathbb{G}_m)$ is isomorphic to the Brauer group of k defined using central simple algebras.

5. $H^1(k, O(q))$ is in bijective correspondence wth the isomorphism classes of quadratic spaces over k.

6. $H^1(k, SO(q))$ is in bijective correspondence wth the isomorphism classes of quadratic spaces over k with a given discriminant.

7. $H^1(k, Sp_{2n}) = 1$.

Example (Kummer sequence): Define $\mu_n = \{x \in \bar{k}^* | x^n = 1\}$. This is a Galois module which sits in the following exact sequence of Galois modules:

$$1 \to \mu_n \to \bar{k}^* \to \bar{k}^* \to 1.$$

The associated Galois cohomology sequence:

$$\begin{aligned} 1 &\to \mu_n(k) \to k^* \xrightarrow{n} k^* \\ &\to H^1(\mathrm{Gal}, \mu_n) \to H^1(\mathrm{Gal}, \bar{k}^*) = 1. \end{aligned}$$

Thus $H^1(k, \mu_n) \cong k^*/k^{*n}$.

Similarly it can be deduced that $H^2(k, \mu_n)$ is isomorphic to the n torsion in the Brauer group of k.

Example (Spin group) To any (non-degenerate) quadratic form q over k, we have the special orthogonal group $SO(q)$, and also a certain 2-fold covering of $SO(q)$, called the *Spin* group associated to the quadratic form q. We have the following exact sequence of algebraic groups:

$$1 \to \mathbb{Z}/2 \to Spin(q) \to SO(q) \to 1.$$

The associated Galois cohomology exact sequence is:

$$\begin{aligned} 1 &\to \mathbb{Z}/2 \to Spin(q)(k) \to SO(q)(k) \to k^*/k^{*2} \\ &\to H^1(k, Spin(q)) \to H^1(k, SO(q)) \to H^2(k, \mathbb{Z}/2). \end{aligned}$$

The mapping $SO(q)(k) \to k^*/k^{*2}$ is called the reduced norm mapping.

The mapping $H^1(k, SO(q)) \to H^2(k, \mathbb{Z}/2) = Br_2(k)$ corresponds to sending a quadratic form q_x to $w_2(q_x) - w_2(q)$ where w_2 is the Hasse-Witt invariant of a quadratic form.

The basic theorem which is the reason for the enormous usefulness of Galois cohomology is the following.

Theorem 1 *1. The set* $H^1(\mathrm{Gal}(K/k), Aut(G)(K))$ *is in bijective correspondence with the set of isomorphism classes of "forms" of* G *over* k*, i.e., sets of isomorphism classes of groups* E *over* k *such that* $G \cong E$ *over* K*.*

2. *(Weil Descent) More generally, for any algebraic variety X over k, the set*

   $H^1(\mathrm{Gal}(K/k), (Aut(X))(K))$ *is in bijective correspondence with the set of isomorphism classes of "forms" of X over k, i.e., sets of isomorphism classes of varieties Y over k such that $X \cong Y$ over K.*

3. *Let V be a vector space over k. Let $\phi_1, \phi_2, \cdots, \phi_r$ be certain tensors in $V^{\otimes a} \otimes V^{*\otimes b}$. Let G be the subgroup of the automorphism group of V fixing the tensors ϕ_i. Then $H^1(\mathrm{Gal}(K/k), G(K))$ is in bijective correspondence with the set of isomorphism classes of tensors $\psi_1, \cdots, \psi_r$ in $V^{\otimes a} \otimes V^{*\otimes b}$ such that there exists $g \in Aut(V)(K)$ such that $g\phi_i = \psi_i$.*

Examples :

1. The set $H^1(k, O(q))$ is in bijective correspondence with the set of quadratic forms over k.

2. $H^1(k, Sp_n) = (1)$.

3. By the Skolem-Noether theorem, the automorphism group of the algebra $M_n(k)$ is $PGL_n(k)$. Hence, $H^1(\mathrm{Gal}(K/k), PGL_n(K))$ is the set of isomorphism classes of central simple algebras of dimension n^2 over k. Define $Br_k^K = \mathrm{Ker}\{Br_k \to Br_K\}$ obtained by sending A to $A \otimes K$. From the exact sequence,

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1,$$

   it follows that there is an injection of $H^1(\mathrm{Gal}(K/k), PGL_n(K))$ into $H^2(\mathrm{Gal}(K/k), K^*)$. The two maps defined here can be combined to produce a map from Br_k^K to $H^2(\mathrm{Gal}(K/k), K^*)$ which can be proved to be an isomorphism.

4. The set of conjugacy classes of maximal tori in a reductive group G with a maximal torus T, normaliser $N(T)$, is $H^1(k, N(T))$. This implies that the tori in a split reductive algebraic group over a finite field k are in bijective correspondence with the conjugacy classes in the Weyl group:

$$\begin{aligned} &H^1(k, T) = 0 \to H^1(k, N(T)) \to \\ &H^1(k, W) \to H^2(k, T) = 0. \end{aligned}$$

Theorem 2 *(Hasse-Minkowski theorem)*

1. *A quadratic form over $\mathbb{Q}$ represents a zero if and only if it represents a zero in $\mathbb{Q}_p$ for all p, and also in $\mathbb{R}$.*
2. *Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they are equivalent at all the places of $\mathbb{Q}$.*

We can interpret the Hasse-Minkowski theorem using Galois cohomology and then the statement naturally generalises for other reductive groups.

Theorem 3 *The natural mapping from $H^1(k, O(q))$ to $\prod_v H^1(k_v, O(q_v))$ is one-to-one, where the product is taken over all the places of k.*

This brings us to the following conjecture, called the Hasse principle, proved by Kneser, Harder, Chunousov.

Conjecture 1 *Let G be a semi-simple simply connected algebraic group over a number field k, then the natural mapping from $H^1(k, G)$ to $\prod_v H^1(k_v, G)$ is one-to-one, where the product is taken over all the places of k.*

It is a consequence of the Hasse principle that if the number field has no real places, then for a semi-simple simply connected group, $H^1(k, G) = 1$. Serre conjectured that this vanishing statement is true for all fields of cohomological dimension 2. This was proved by Eva-Bayer and Parimala for all classical groups.