Lecture Notes to Linear Algebraic Groups

Winter 2021-2022, Technion IIT

Typed by Elad Tzorani

A cat.

Last updated November 3, 2021

Contents

Preface

Technicalities

These aren't formal notes related to the course and henceforward there is *absolutely no guarantee* that the recorded material is in correspondence with the course expectations, or that these notes lack any mistakes.
In fact, there probably are mistakes in the notes! I would highly appreciate if any comments or corrections were sent to me via email at tzorani.elad@gmail.com.
Elad Tzorani.

Grade

The course grade will consist of the following.

- 60% for homework
- 40% for giving lectures on more advanced topics at the end of the semester

Chapter 1

Linear Algebraic Groups

1.1 Preliminaries

1.1.1 Motivation & Historical Background

Linear Algebraic Groups From Differential Equations

Algebraic groups developed from the study of Lie groups. The latter were studied by Sophus Lie around 1870 in the context of differential equations. Lie groups can describe symmetries of solutions of differential equations; e.g. solutions of $\nabla y = 0$ are *harmonic functions* and one is interested in linear isomorphisms $g\colon \mathbb{R}^n \to \mathbb{R}^n$ such that $\Delta(y) = 0$ implies $\Delta(y \circ g) = 0$. Lie noticed that such g form a group $\mathcal{O}_n(\mathbb{R}) \coloneqq \left\{ g \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; g^T g = I_n \right\}$. Such groups for operators different than Δ are smooth manifolds with smooth group actions, called *Lie groups.* One of Lie's motivation was to have Galois theory for differentiable equations. It had already been known that in order to find roots of polynomials one uses the symmetries of field extensions.
Around 1880, Picard looked at differentiable equations of the form

$$\frac{(\mathrm{d}y)^{n\,n}}{\mathrm{d}x} + p_1(x)\frac{\mathrm{d}y^{n-1}}{(\mathrm{d}x)^{n-1}} + \ldots + p_n(x)\,y = 0$$

for p_i rational functions. The solution space for such an equation is the n-dimensional space

$$\mathrm{Span}\left\{ y_1(x), \ldots, y_n(x) \right\}.$$

Picard looked at a subgroup $G \leq \mathrm{GL}_n(\mathbb{R})$ which preserves the algebraic dependencies of the y_i (i.e. preserves polynomials $p \in \mathbb{R}_n[x]$ for which $p(y_1(x), \ldots, y_n(x)) = 0$). These were the first treatments of algebraic groups.
Around 1870-1900, Mauren took homogeneous rational functions $f\colon \mathbb{C}^n \to \mathbb{C}$ (such as $f(x_1, \ldots, x_n) = \sum_{i=1}^n x_i^2$ for which $G_f = \mathcal{O}_n(\mathbb{C})$) and studied the structure of

$$G_f \coloneqq \left\{ g \in \mathrm{GL}_n(\mathbb{C}) \mid f \circ g = f \right\}.$$

One can take f to be any quadratic form, e.g.

$$\mathrm{Sp}_{2n}(\mathbb{C}) = \left\{ g \in \mathrm{GL}_{2n}(\mathbb{C}) \;\middle|\; g^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} g = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \right\}$$

is such group. Such groups are called *classical groups.*
Mauren looked at the tangent space of such group. His motivation was his interest in Hilbert's 14^{th} problem: Given $g \in G \leq \mathrm{GL}_n(\mathbb{C})$ we can consider g as a map $\mathbb{C}^n \to \mathbb{C}^n$. Considering the action $G \curvearrowright \mathbb{C}[x_1, \ldots, x_n]$ on the coefficient, the problem is understanding the invariant space of this action. E.g. the invariant space of S_n are *symmetric polynomials.*

Later Developments

The field of Lie groups gave great success. Semisimple Lie groups have complete combinatorical classification due to Cartan and Killing. This is considered one of the greatest achievements in mathematics.

Chevalley found out the every semisimple Lie group is defined by polynomials in integer coefficients, circa 1940. This led to the definition of algebraic groups and a new goal: to algebrize Lie theory and develop tools to study smooth symmetric "without analysis" and over more general fields. This should form a bridge between continuous groups and finite groups. Chevalley used in his studies of the subject the formal expression

$$\exp(X) = \sum_{n=0}^{\infty} \frac{1}{n!} X^n$$

and required $\operatorname{char}(\mathbb{F}) = 0$. Later Kolchin returned to Picard's ideas and developed a differential Galois theory over a general field.

Modern Developments

From 1950 onwards, many mathematicians developed the study of algebraic groups, which was possible thanks to advances in algebraic geometry. Some of the advances of the field are the following.

1. The classification of finite simple groups. Most of these groups are of "Lie type", which are of the form $\mathrm{Sp}_{2n}(\mathbb{F}_q)$.
2. Results on p-adic groups. For example, Bruhat-Tits buildings are homogeneous spaces with p-adic group actions and which are "non-archimedean" analogues to classical symmetric spaces.
3. Results in number theory.

The Langlands Program

The Laglands program, circa 1960, tries to study properties in number theory through the study of groups. There are analogues to Riemann's zeta function which one hopes all arise from group actions in the following way. Taking an algebraic group G, one looks at *automorphic spaces* V with $G(\mathbb{R})$ and $G(\mathbb{Q}_p)$ actions which commute with each other, for some groups $G(\mathbb{R}), G(\mathbb{Q}_p)$ over the respective fields.

1.1.2 Definitions & Course Goals

What are Algebraic Groups?

Write $\mathbb{F}$ for a field, and write $M_n(\mathbb{F}) \cong \mathbb{F}^{n^2}$ for the space of $n \times n$ matrices over $\mathbb{F}$.

Definition 1.1.1 (Affine Algebraic Group). A subset $G \leq M_n(\mathbb{F})$ closed under multiplication and inverse is called an *affine algebraic group* over $\mathbb{F}$ if there are $f_1, \ldots, f_k \in \mathbb{F}\left[\{x_{i,j}\}_{i,j\in[n]}\right]$ such that

$$G = \{A \in M_n(\mathbb{F}) \mid f_1(A) = \ldots = f_k(A) = 0\}.$$

Example 1. $\mathrm{SL}_n(\mathbb{F})$ is n affine algebraic group. The determinant,

$$\det(X) = \sum_{\sigma \in S_n} (-1)^{\operatorname{sgn}(\sigma)} x_{1,\sigma(1)} \cdot \ldots \cdot x_{n,\sigma(n)},$$

is a polynomial and $\mathrm{SL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \det(A) - 1 = 0\}$.

Example 2. Let $Q \in M_n(\mathbb{F})$ and denote

$$\mathcal{O}_Q(\mathbb{F}) \coloneqq \left\{A \in \mathrm{GL}_n(\mathbb{F}) \;\middle|\; A^t Q A = Q\right\}.$$

Taking $Q = I_n$ one gets $\mathcal{O}_Q(\mathbb{R}) = \mathcal{O}_n(\mathbb{R})$. More generally, matrix multiplication is polynomial and one can write $A^t Q A - Q = 0$ as a polynomial equation in the coefficients of A. We explain the condition $A \in \mathrm{GL}_n(\mathbb{F})$ later.

Example 3. Let $N \subseteq M_n(\mathbb{F})$ be the subset of upper-triangular matrices with 1 on the diagonal. This is an algebraic group with polynomial conditions $x_{i,j} = 0$ for $i > j$ and $x_{i,i} = 1$ for all $i \in [n]$. One has $N \cong \mathbb{F}^{\frac{n(n-1)}{2}}$ as vector space, but this doesn't remember the group structure.

Example 4. The vector space $\mathbb{F}^n$ with addition is an algebraic group. We have

$$V \coloneqq \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 & * \\ 0 & & & & * \\ \vdots & & \ddots & & \vdots \\ & & & & * \\ 0 & & \cdots & & 1 \end{pmatrix} \in M_{n+1}(\mathbb{F}) \right\} \cong \mathbb{F}^n.$$

One denotes $G_a(\mathbb{F}) \coloneqq (\mathbb{F}, +)$ and calls this *the additive group over* $\mathbb{F}$.

Remark 1.1.2. One has

$$\mathrm{GL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det(A) \neq 0\} \cong \left\{ \begin{pmatrix} A & 0 \\ 0 & a \end{pmatrix} \in M_{n+1}(\mathbb{F}) \;\middle|\; \det(A) \cdot a = 1 \right\}$$

and a bijection $A \leftrightarrow \begin{pmatrix} A & 0 \\ 0 & \det(A)^{-1} \end{pmatrix}$, but this looks weird. We then want the definition to be more general and capture groups that are isomorphic to what we defined as affine algebraic groups. We do that later in the course.

Example 5. Every finite group G is an algebraic group. One has an inclusion $G \hookrightarrow S_n$, and S_n is an algebraic group where σ is considered as $(x_{i,j})_{i,j\in[n]}$ with $x_{i,\sigma(i)} = 1$ and $x_{i,j} = 0$ for any other $i, j \in [n]$.

Exercise 1. Every finite subset $M_n(\mathbb{F})$ is an algebraic set, in the sense that it's defined by the vanishing of polynomials.

To study properties of algebraic groups, one needs to use tools from algebraic geometry. Here there are two possible difficulties:

1. One needs to ask what generality is to be worked with. With our current definition it is difficult to use strong algebro-geometric tools, but with "too general" definitions it is more difficult to look at simple examples.

2. One should decide how much they want to rely on geometric results as facts and how much is to be proved.

Our answer to the latter question is proving things at the beginning of the course and later on taking more things as facts. For the first difficulty...you'll see as we go.

A Course Overview

During the course we plan to go over the following.

- Basic algebraic geometry.
- General structure properties of algebraic groups. For example, a generalization of Jordan's decomposition to GL_n.
- Generalization of the notion of an algebraic group.
- Study of algebraic groups by looking at algebraic groups over the Galois closure and via Galois theory.
- The classification of reductive groups over algebraically closed fields. An algebraic version of the Cartan-Killing classification.

1.1.3 Preliminary Algebraic Geometry

Embedded $\mathbb{F}$-Affine Varieties

Notation 1.1.3. Denote $A_n \coloneqq \mathbb{F}[x_1, \ldots, x_n]$.

Definition 1.1.4. For $C \subseteq A_n$ define

$$V(C) \coloneqq \{p \in \mathbb{F}^n \mid \forall f \in C \colon f(p) = 0\} \subseteq \mathbb{F}^n.$$

A set of this form is called an *embedded $\mathbb{F}$-Affine Variety.*

Definition 1.1.5. For $S \subseteq \mathbb{F}^n$ define

$$I(S) \coloneqq \{f \in A_n \mid \forall p \in S \colon f(p) = 0\}.$$

Exercise 2. For $S \subseteq \mathbb{F}^n$ one has $I(S) \trianglelefteq A_n$.

Example 6. One has $I(\varnothing) = A_n$ and whenever $\mathbb{F}$ is infinite one has $I(\mathbb{F}^n) = \{0\}$.

Example 7. For $I = \left\{x_1^2 - x_2, x_1^3 - x_3\right\}$ one has $V(I) = \left\{\left(x, x^2, x^3\right) \;\middle|\; x \in \mathbb{F}\right\}$ which one calls the *twisted cubic* over $\mathbb{F}$

Proposition 1.1.6. *One notices that for $S \subseteq \mathbb{F}^n$ and $C \subseteq A_n$ we have*

$$\begin{aligned} S &\subseteq V(I(S)) \\ C &\subseteq I(V(C)). \end{aligned}$$

Definition 1.1.7 (The Zariski Topology). The *Zariski topology* on $\mathbb{F}^n$ is the topology given by taking sets of the form $V(C)$ for $C \subseteq A_n$ as the closed subsets.

Exercise 3. Check that the above definition gives a well-defined topology.

Exercise 4. For $S \subseteq \mathbb{F}^n$ one has $\overline{S} = V(I(S))$.

Example 8. Consider the case $n = 1$. Then closed subsets of $\mathbb{F}$ are sets of the form $V(C)$ for $C \subseteq A_n$. If C contains a nonzero polynomial, $V(C)$ is finite, and otherwise $V(C) = \mathbb{F}$. We get that the nontrivial closed sets are exactly the finite subsets of $\mathbb{F}^n$.

Remark 1.1.8. $\mathbb{F}^n$ with the Zariski topology is always *quasi-compact*, meaning it's compact but not Hausdorff.

Theorem 1.1.9 (Hilbert's Basis Theorem). *Every ideal $I \trianglelefteq A_n$ is finitely-generated.*

Proof. We prove the statement by induction on $n \in \mathbb{N}$. The case $n = 0$ is trivial since $\mathbb{F}$ is a field. Assume the statement is true for $n - 1$, we show it for n. Write $A_n \cong A_{n-1}[x_n]$ and assume $I \trianglelefteq A_n$ is nonzero. Choose $f_1 \in I \setminus \{0\}$ of minimal degree and write $d_1 \coloneqq \deg_{A_{n-1}} f_1$. If $(f_1) \neq I$, choose $f_2 \in I \setminus (f_1)$ of minimal degree $d_2 \coloneqq \deg_{A_{n_1}}(f_2)$. Continue this way to get f_i with $d_i \coloneqq \deg_{A_{n-1}}(f_i)$ and $d_1 \leq d_2 \leq d_3 \leq \ldots$.
Assume that this doesn't end a finite point (for otherwise we're done). Denote by $a_i \in A_{n-1}$ the leading coefficient of f_i. By assumption, $I' \coloneqq (a_1, \ldots, a_i, \ldots) \trianglelefteq A_{n-1}$ is finitely-generated. We can then write $I' = (a_1, \ldots, a_h)$ for some $h \in \mathbb{N}$. Then

$$a_{h+1} = x_1 a_1 + \ldots + x_h a_h$$

for some $x_1, \ldots, x_h \in A_{n-1}$. Let

$$g \coloneqq f_{h+1} - \sum_{i \in [h]} x_i \cdot f_i \cdot x^{d_{h+1} - d_i} \in I.$$

The coefficient of $x^{d_{h+1}}$ in g vanishes so $\deg(g) < d_{h+1}$ and $g \in (f_1,\ ldots, f_h)$. Then also $f_{h+1} \in (f_1, \ldots, f_h)$, in contradiction. ∎

Definition 1.1.10 (Noetherian Topological Space). A topological space X is called *Noetherian* if every decreasing sequence of closed subsets stabilises.

Corollary 1.1.11. *$\mathbb{F}^n$ with the Zariski topology is Noetherian.*

Proof. Let $(X_i)_{i\in\mathbb{N}_+} \subseteq \mathbb{F}^n$ be a decreasing sequence of closed subsets, and for every i denote $I_i \coloneqq I(X_i)$. Then $X_i = V(I_i)$. We get $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Denote $I = \bigcup_{i\in\mathbb{N}_+} I_i$. By Theorem 1.1.9 we have $I = (f_1, \ldots, f_k)$ for some $k \in \mathbb{N}_+$. Then $f_1, \ldots, f_k \in I_m$ for some $m \in \mathbb{N}_+$. We get $I = I_m = I_{m+1} = \ldots$ and $X_m = X_{m+1} = X_{m+2} = \ldots$, as required. ∎

Exercise 5. Every closed subspace $X \subseteq \mathbb{F}^n$ is quasi-compact.

Example 9. Consider $xy \in \mathbb{F}[x, y]$. $V(x, y)$ is connected, but we would like to say it has two components. E.g. if $\mathbb{F} = \mathbb{R}$, the set $V(x, y)$ is the union of two perpendicular axes. This leads to the following definition.

Definition 1.1.12 (Irreducible Topological Space). A topological space X is *irreducible* if there aren't strict closed subsets $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$.

Exercise 6. An irreducible Hausdorff topological space is a point.

Exercise 7. In a Noetherian space X there are finitely many maximal irreducible subsets $X_1, \ldots, X_k$, and $X = \bigcup_{i\in[k]} X_i$.

Proposition 1.1.13. *An algebraic variety $V \subseteq \mathbb{F}^n$ is irreducible if and only if $I(V)$ is prime.*

Proof. Assume V is irreducible. Let $f_1, f_2 \in A_n$, such that $f_1 f_2 \in I(V)$, we want to show $f_1 \in I(V)$ or $f_2 \in I(V)$. We have $V \subseteq V(f_1 f_2) = V(f_1) \cup V(f_2)$. Now $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ and by irreducibility $V = V \cap V(f_i)$ for $i \in [2]$, in which case $V \subseteq V(f_i)$ and therefore $f_i \in I(V)$.
The other direction is left as an exercise. ∎

Example 10. Consider $G \coloneqq \mathrm{GL}_1(\mathbb{F}) \cong \mathbb{F}^\times \subseteq \mathbb{F}$. We have $V(x-1) = \{1\}$ and similarly $V\left((x-1)^2\right) = \{1\}$. If $\mathbb{F} = \mathbb{R}$, one has $V\left(x^5 - 1\right) - 1 = \{1\}$ and one gets the same subgroup of G. However, over $\mathbb{F} = \mathbb{C}$ the group $V\left(x^5 - 1\right)$ is the roots of unity of order 5.

Example 11. Let $V \subseteq \mathbb{F}^n$ be closed, and for $f \in A_n$ define

$$V_f \coloneqq \{x \in V \mid f(x) \neq 0\} = V \setminus V(f).$$

This is open in V and such a set is called a *principal open set*. Every open set U is a finite union of such sets, so the principal open sets form a basis for the Zariski topology:
If U is open in V let $W \coloneqq V \setminus U$ so that there are $(f_i)_{i\in[k]} \subseteq A_n$ for which

$$V \setminus U = V \cap W = V(f_1, \ldots, f_k)$$

so

$$U = \bigcup_{i\in[k]} V_{f_i}.$$

We sometimes want to think of V_f as closed sets. This can be done by considering

$$\tilde{V}_f \coloneqq \left\{(v, y) \;\middle|\; \begin{smallmatrix} v\in\mathbb{F}^n \\ y\in\mathbb{F} \\ f(v)\cdot y = 1 \end{smallmatrix}\right\} \subseteq \mathbb{F}^{n+1}.$$

There's a clear bijection $V_f \xrightarrow{\sim} \tilde{V}_f$.

Definition 1.1.14 (Morphism of Embedded Algebraic Varieties). For embedded algebraic varieties $V \subseteq \mathbb{F}^n$ and $W \subseteq \mathbb{F}^m$, a *morphism* $\phi\colon V \to W$, called also a *regular map* is a map of the form

$$\phi(x) = (f_1(x), \ldots, f_m(x))$$

for $(f_i)_{i\in[m]} \subseteq A_n$.

Example 12. The map

$$\phi\colon \mathbb{F}^2 \to \mathbb{F}^2 \, (x, y) \qquad\qquad \mapsto (xy, y)$$

is a regular map.

Exercise 8. A regular map is continuous in the Zariski topology.

Definition 1.1.15. A *regular function* on an embedded algebraic variety V over $\mathbb{F}$ is a regular map $V \to \mathbb{F}$.

Remark 1.1.16. Regular functions on V are of the form $f|_V$ for $f \in A_n$. We can think of these as elements of $\mathbb{F}[V] \coloneqq A_n / I(V)$.