Algebraic Groups

Lecturer: Tamás Szamuely
Typed by: Szabolcs Mészáros

March 9, 2017

Remark. This is the live-texed notes of Algebraic Groups course held by Tamás Szamuely in the winter of 2017. Any mistakes and typos are my own.

First Lecture, 12th of January

Literature:

- Borel: Linear Algebraic Groups
- Humphreys: Linear Algebraic Groups
- Springer: Linear Algebraic Groups
- Milne: Introduction to Algebraic Groups
- Grothendieck: SGA3
- Waterhouse: Introduction to Affine Group Schemes
- notes on the homepage of the lecturer

The topic of algebraic groups, especially affine algebraic groups lie in the intersection of group theory, algebraic geometry, Lie theory and of linear algebra.

Setup: Through the notes $\mathbb{k}$ will denote an algebraically closed field.

The zero locus $V(I) = \{p \in \mathbb{A}^n \mid f(p) = 0, \ \forall f \in I\} \subseteq \mathbb{A}^n = \mathbb{k}^n$ of an ideal $I \subseteq \mathbb{k}[x_1, \dots, x_n]$ will be called an affine variety where irreducibility is not assumed! $I(X) = \{f \in \mathbb{k}[x_1, \dots, x_n] \mid f(p) = 0, \ \forall p \in X\}$ stands for the vanishing ideal of an affine variety $X \subseteq \mathbb{A}^n$. Recall that by the Nullstellensatz, there is a bijection between radical ideals of $\mathbb{k}[x_1, \dots, x_n]$ and affine varieties i.e. closed subsets of $\mathbb{A}^n$ (with the above terminology).

Omitted: We got a reminder on the definition of Zariski topology, irreducibility of a variety, on the decomposition into finitely many irreducible components by Noetherian descent, on the definition of morphisms between affine varieties, products of affine varieties,

Definition 0.1. An affine algebraic group is an affine variety G equipped with a group structure such that the multiplication $m : G \times G \to G$ and the inversion $i : G \to G$ are morphisms of affine varieties.

Example 0.2.

1. the additive group $\mathbb{G}_a$ i.e. $\mathbb{A}^1$ with the addition of $\mathbb{k}$,
2. the multiplicative group $\mathbb{G}_m$ i.e. $\mathbb{A}^1 \backslash \{0\}$ with the multiplication of $\mathbb{k}$, (note that $\mathbb{A}^1 \backslash \{0\}$ can be embedded into $\mathbb{A}^2$ as a closed set)

3. let $(n, \mathrm{char}\Bbbk) = 1$ and consider the closed subvariety $\mu_n := \{x \in \Bbbk \mid x^n = 1\} = V(x^n - 1) \subseteq \mathbb{A}^1$ with its multiplication, (if $(n, \mathrm{char}\Bbbk) \neq 1$ then the natural analog of this object is a non-reduced scheme)

4. the general linear group $GL_n = \{A \in \Bbbk^{n\times n} \mid \det A \neq 0\}$ that can be made into an affine variety by taking $V(\det A \cdot x_{n^2+1} - 1) \subseteq \Bbbk^{n\times n+1}$,

5. the special linear group $SL_n = \{M \in \Bbbk^{n\times n} \mid \det(M) = 1\}$.

Proposition 0.3. *Let $\Bbbk$ be an affine algebraic group.*

1. *All connected components of G are irreducible. Consequently, G has only finitely many connected components.*

2. *The connected component G° of the identity is an algebraic group. In fact, it is a normal subgroup of finite index, and its cosets are the connected components of G.*

Remark 0.4. We only use that G is a topological group with finitely many components.

Proof. Let $G = X_1 \cup \cdots \cup X_n$ be the decomposition of G into irreducible components. By definition, there is an $x \in X_1 \setminus \cup_{j>1} X_j$. Note that there is only one component of G passing through x. Let $g \in G$ be an arbitrary fixed element and consider the morphism $G \to G$, $y \mapsto gx^{-1}y$. This is a homeomorphism and it maps x into g where g was arbitrary hence there is only one irreducible component passing through every point of G. The claim follows.

For the second part, consider the homeomorphism $y \mapsto gy$ for a fixed $g \in G$. Then gG° is the connected component of g for all $g \in G$. Hence, if $g \in G^\circ \cap gG^\circ$ then $G^\circ = gG^\circ$. Therefore, G° is closed under multiplication and under inverse. Moreover, $gG^\circ g^{-1} = G^\circ$ for all $g \in G$ hence it is a normal subgroup. □

1 Abelian varieties

Proposition 1.1. *If G is a connected projective algebraic group (i.e. a projective variety with a group structure consisting of morphisms of projective varieties) then it is commutative.*

Definition 1.2. A connected projective algebraic group is called an *abelian variety*.

Example 1.3. For projective algebraic groups:

1. Elliptic curves: defined as $V(y^2z - x^3 - px^2z - qz^3) \subseteq \mathbb{P}^2$ where $4p^3 + 27q^2 \neq 0$. These are all the projective algebraic groups in dimension one.

2. Let X be a smooth projective curve, the group $\mathrm{Pic}^\circ(X)$ has a structure of a projective variety such that it is an projective algebraic group, called the Jacobian of X. Its dimension is the genus of the curve.

Lemma 1.4. (Rigidity Lemma) *Let U, V, W be irreducible quasi-projective varieties, V projective. Assume given a morphism $f : V \times W \to U$ and points $u_0 \in U$, $v_0 \in V$ and $w_0 \in W$ such that*

$$f(V \times \{w_0\}) = \{u_0\} = f(\{v_0\} \times W)$$

Then f must be constant.

Proof of Proposition 1.1 by Lemma 1.4. Let $i : G \to G$ be the inversion of the group. It is enough to prove that it is a group homomorphism since that is equivalent to the commutativity of G. Let φ be the commutator map i.e.

$$\varphi(g_1, g_2) = (g_1g_2)^{-1}g_2g_1$$

This map satisfies the condition of Lemma 1.4: $f(G \times \{1\}) = \{1\} = f(\{1\} \times G)$ hence it is identically 1. □

Proof of Lemma 1.4. Recall that V an irreducible projective variety is universally closed i.e. for any variety W the projection $p_2 : V \times W \to W$ is closed. Consequently, when we apply it for the graph of a morphism, we obtain that the image of a an irreducible projective variety is closed. In particular, any regular function on an irreducible projectve variety is constant.

Let $U_0 \subseteq U$ be an affine open neighborhood of $u_0 \in U$ and consider the closed subset $f^{-1}(U\backslash U_0) \subseteq V \times W$. By the previous paragraph, $Z := p_2\big(f^{-1}(U\backslash U_0)\big) \subseteq W$ is closed. By the definition,

$$W\backslash Z = \{w \in W \mid f(V \times \{w\}) \subseteq U_0\}$$

and it is an open subset in W containing w_0, hence dense. However, $f(V \times \{w\})$ is always a one-point set as U_0 is affine and $V \times \{w\}$ is an irreducible projective variety, hence we may apply the previous paragraph. In fact, this one-point set is always $\{u_0\}$ as $(v_0, w) \in V \times \{w\}$ and $f(v_0 \times W) = \{u_0\}$. Therefore, f is constant u_0 on $V \times W\backslash Z$ but that is a dense subset of $V \times W$. The claim follows. □

2 General cases

Theorem 2.1. *(Chevalley) A general algebraic group G (that is a group object among separated schemes of finite type over $\Bbbk$) has a largest affine normal closed subgroup G_{aff} and G/G_{lin} is an abelian variety.*

Theorem 2.2. *(Rosenlicht) G has a largest affine quotient G^{aff} and the kernel G_{ant} lies in the center of G, and it has no non-constant regular functions.*

Goal: Every affine algebraic group is a *linear algebraic group* i.e. it can be embedded as a closed subgroup of GL_n.

Omitted: Reminder on the coordinate ring $\mathcal{A}_X$ of an affine variety X: a finitely generated reduced $\Bbbk$-algebra, and the induced homomorphisms on these algebras that give isomorphism between the hom-spaces. In short, the category of finitely generated reduced $\Bbbk$-algebras is anti-equivalent to the category of affine varieties. Consequently, X is isomorphic to a closed subvariety of Y if and only if there exists an algebra surjection $\mathcal{A}_Y \to \mathcal{A}_X$. Recall that $\mathcal{A}_{X\times Y} \cong \mathcal{A}_X \otimes_{\Bbbk} \mathcal{A}_Y$ via the multiplication of the functions (where the Nullstellensatz is applied at the proof of injectivity).

Definition 2.3. The group structure on an affine algebraic group G induces extra structure on $\mathcal{A}_G$ called a *Hopf algebra* structure:

- the multiplication $m : G \times G \to G$ induces a map $\Delta : \mathcal{A}_G \to \mathcal{A}_G \otimes \mathcal{A}_G$ called the comultiplication,
- the unit $\{e\} \hookrightarrow G$ induces a map $\varepsilon : \mathcal{A}_G \to \Bbbk$ called the counit,
- the inverse $i : G \to G$ induces a map $i : \mathcal{A}_G \to \mathcal{A}_G$ called the coinverse or antipode.

Moreover, the group axioms imply axioms for Δ, ε and i:

- associativity: $m \circ (\mathrm{id} \times m) = m \circ (m \times \mathrm{id})$ implies coassociativity: $(\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta$
- unitality: $m \circ (\mathrm{id} \times e) = \mathrm{id} = m \circ (e \times \mathrm{id})$ implies counitality: $(\mathrm{id} \times \varepsilon) \circ \Delta = \mathrm{id} = (\varepsilon \times \mathrm{id}) \circ \Delta$
- and the inverse property: $m \circ (\mathrm{id} \times i) \circ \mathrm{diag} = e = m \circ (i \times \mathrm{id}) \circ \mathrm{diag}$ implies the compatibility of the antipode $m_{\mathcal{A}} \circ (\mathrm{id} \times i) \circ \Delta = \varepsilon = m_{\mathcal{A}} \circ (i \times \mathrm{id}) \circ \Delta$.

Example 2.4. Hopf algebra structure on algebraic groups:

1. on $\mathcal{A}_{\mathbb{G}_a} = \Bbbk[x]$ it is given by $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$, $i(x) = -x$,

2. on $\mathcal{A}_{\mathbb{G}_m} = \Bbbk[x, x^{-1}]$ it is given by $\Delta(x) = x \otimes x$, $\varepsilon(x) = 1$, $i(x) = x^{-1}$,
3. on $\mathcal{A}_{GL_n} \cong \Bbbk[x_{11}, \ldots, x_{nn}, \det(X)^{-1}]$ it is given by $\Delta(x_{ij}) = \sum_k x_{ik} \otimes x_{kj}$, $\varepsilon(x_{ij}) = \delta_{ij}$, $[i(x_{ij})]_{i,j} = [x_{ij}]^{-1}$.

Remark 2.5. If G is an affine algebraic group then $\mathcal{A}_G$ is a Hopf algebra. If R is a $\Bbbk$-algebra then $\mathrm{Hom}_{\Bbbk}(\mathcal{A}_G, R)$ has a group structure. In particular, for $R = \Bbbk$ it is the group structure on G. In fact, $\Phi_G : R \mapsto \mathrm{Hom}(\mathcal{A}_G, R)$ is a (representable) contravariant functor from $\Bbbk$-algebras to groups. So we could define Φ_G as a contravariant functor from $\Bbbk$-algebras to groups which is isomorphic to the functor $R \mapsto \mathrm{Hom}(\mathcal{A}_G, R)$ as a functor from $\Bbbk$-algebras to sets (!).

Second Lecture, 19th of January

Theorem 2.6. *Let G be an affine algebraic group. Then there exists an embedding $G \hookrightarrow GL_n$ with closed image.*

Proof. The idea is the following: Let G be a finite group and $\Bbbk[G]$ its group algebra, a finite dimensional $\Bbbk$-algebra, and $G \hookrightarrow GL(\Bbbk[G]) \cong GL_n(\Bbbk)$ is the left regular representation. Then its image is finite hence closed. In the case of non-finite algebraic groups, $\mathcal{A}_G$ is more suitable instead of $\Bbbk[G]$.

Let $g \in G$ fix and consider the map $R_g : G \to G$ defined as $x \mapsto xg$. This is an automorphism of G as a $\Bbbk$-variety. Indeed, it is a morphism of algebraic varieties as the group multiplication is a morphism too. Moreover, it is also invertible as $R_g R_{g^{-1}} = \mathrm{id}$. The map R_g induces a $\Bbbk$-algebra automorphism $\rho_g \in GL(\mathcal{A}_G)$ with respect to the pointwise multiplication of $\mathcal{A}_G$. This way we got a homomorphism $G \to GL(\mathcal{A}_G)$ by $g \mapsto \rho_g$.

Lemma 2.7. *Let $V \subseteq \mathcal{A}_G$ be a $\Bbbk$-linear subspace. Then*

1. *$\rho_G(V) \subseteq V$ for all $g \in G$ if and only if $\Delta(V) \subseteq V \otimes \mathcal{A}_G$ where Δ is the comultiplication of $\mathcal{A}_G$ defined last time.*
2. *If $\dim_{\Bbbk} V < \infty$ then there exists a $\Bbbk$-linear subspace $W \subseteq \mathcal{A}_G$ such that $V \subseteq W$, $\dim_{\Bbbk} W < \infty$ and $\rho_g(W) \subseteq W$ for all $g \in G$.*

Proof. First, assume that $\Delta(V) \subseteq V \otimes \mathcal{A}_G$. Given $f \in V$ there exist $f_i \in V$, $g_i \in \mathcal{A}_G$ such that $\Delta(f) = \sum_i f_i \otimes g_i$. Then

$$\rho_g(f)(h) = f(hg) = \sum_i f_i(h) g_i(g) \tag{2.1}$$

for all $g \in G$. Hence, $\rho_g(f) = \sum_i g_i(g) f_i \in V$ as V is spanned by f_i's by the assumption.

Conversely, assume that $\rho_g(V) \subseteq V$ for all $g \in G$. Let $\{f_i \mid i \in I\}$ be a basis of V. Choose elements $\{g_j \mid j \in J\}$ extending the set of f_i's to a $\Bbbk$-basis of $\mathcal{A}_G$. Then, writing $\Delta(f)$ using this basis we obtain

$$\Delta(f) = \sum_i f_i \otimes u_i + \sum_j g_j \otimes v_j$$

for some $u_i, v_j \in \mathcal{A}_G$. Hence, as before

$$(\rho_g f)(h) = \sum_i f_i(h) u_i(g) + \sum_j g_j(h) v_j(g)$$

where the second summand is zero for all $g \in G$ by $\rho_g(V) \subseteq V$. Therefore, $v_j = 0$ for all j.

In the case of the second statement, it is enough to treat that case when $\dim_{\Bbbk} V = 1$. Let $V = \mathrm{Span}(f)$. Define $f_i \in \mathcal{A}_G$ and $g_i \in \mathcal{A}_G$ for all i by the formula $\Delta(f) = \sum_{i \in I} f_i \otimes g_i$. Let $W' := \mathrm{Span}(f_i \mid i \in I)$, a finite dimensional subspace. Then $\rho_g(f) \in W'$ for all $g \in G$ by Equation 2.1. Now, take $W := \mathrm{Span}(\rho_g(f) \mid g \in G) \subseteq W'$. This already satisfies all the required properties. ∎

To finish the proof of the theorem, we have to find a finite dimensional subspace of $\mathcal{A}_G$ that is G-stable and where G acts faithfully. Note that $\mathcal{A}_G$ is a finitely generated $\Bbbk$-algebra, hence, there exists a finite dimensional $\Bbbk$-subspace $V \subseteq \mathcal{A}_G$ such that $\dim_{\Bbbk} V < \infty$ such that V generated $\mathcal{A}_G$ as a $\Bbbk$-algebra. We may apply part 2 of Lemma 2.7, there is a $\Bbbk$-subspace $W \supseteq V$ such that $\dim_{\Bbbk} W < \infty$ and $\rho_g(W) \subseteq W$ for all $g \in G$. Let $f_1, \dots, f_n$ be a $\Bbbk$-basis in W.

We may also apply part 1 of Lemma 2.7, hence there are functions $a_{ij} \in \mathcal{A}_G$ such that $\Delta(f_i) = \sum_j a_{ij} \otimes f_j$ for all i, i.e. $\rho_g(f_i) = \sum_j a_{ij}(g) f_j$, in other words $[a_{ij}(g)]_{i,j}$ is the matrix of ρ_g in the basis $\{f_i\}_i$. Together, these give a map $\Phi : G \to \mathbb{A}^{n^2}$ by $g \mapsto [a_{ij}(g)]_{i,j}$. Moreover, $\Phi(g)$ is an invertible matrix for all $g \in G$, i.e. $\mathrm{Im}(\Phi) \subseteq GL_n$. We need to prove that Φ is a closed embedding, equivalently, that $\Phi^* : \mathcal{A}_{GL_n} \to \mathcal{A}_G$ is a surjective map. Last time, we have seen in Example 2.4 that $\mathcal{A}_{GL_n} = \Bbbk[x_{11}, \dots, x_{nn}, \det(X)^{-1}]$. In these terms, $\Phi^*(x_{ij}) = a_{ij}$. Moreover, by Eq. 2.1, $f_i(g) = \sum_j f_j(1) a_{ij}(g)$ i.e. $f_i = \sum_j f_j(1) a_{ij}$. As f_i's generate $\mathcal{A}_G$ as an algebra, by the previous equation also the elements $\{a_{ij}\}_{i,j}$ generate $\mathcal{A}_G$, hence the map is indeed surjective. □

Corollary 2.8. *Suppose that $H \subseteq G$ is a closed subgroup. Then there exists a closed embedding $G \hookrightarrow GL(W)$ where $\dim_{\Bbbk} W < \infty$ such that H is the stabilizer of a subspace $W_H \subseteq W$.*

Proof. Let $I_H \subseteq \mathcal{A}_G$ be the vanishing ideal of H. We may modify the previous proof so that the $\Bbbk$-basis $\{f_i \mid i \in I\}$ of $\mathcal{A}_G$ is chosen so that some finite subset $f_{i_1}, \dots, f_{i_k}$ form a system of generators of I_H. Let $W_H := W \cap I_H$, this will satisfy the statement. Indeed, for $g \in G$, $\rho_g(I_H) \subseteq I_H$ is equivalent to $g \in H$ which is equivalent to $\rho_g(W_H) \subseteq W_H$. □

3 Jordan decomposition

Definition 3.1. Let V be a finite dimensional $\Bbbk$-vector space, an endomorphism $g \in \mathrm{End}(V)$ is semisimple, if V has a basis of eigenvectors of g. Similarly, it is called nilpotent if there exists an $m > 0$ such that $g^m = 0$.

Proposition 3.2. *(Additive Jordan Decomposition) For any $g \in \mathrm{End}(V)$ there are $g_s, g_n \in \mathrm{End}(V)$ such that $g = g_s + g_n$, g_s is semisimple, g_n is nilpotent and $g_s g_n = g_n g_s$.*

Corollary 3.3. *(Multiplicative Jordan Decomposition) For any $g \in GL(V)$ where $\dim V < \infty$ there are elements $g_s, g_u \in GL(V)$ such that g_s is semisimple, g_u is unipotent (i.e. $g - 1$ is nilpotent) and $g = g_s g_u = g_u g_s$.*

Proof. Define g_s as above, it has nonzero eigenvalues as $g \in GL(V)$. Therefore, $g_s \in GL(V)$ so we may take $g_u := \mathrm{id} + g_s^{-1} g_n$. □

Lemma 3.4. *In the above decompositions, g_s and hence g_n and g_u are uniquely determined.*

Proof. If $g = g_s' + g_n' = g_s + g_n$ where $g_s' g_n' = g_n' g_s'$ then $g_s'(g - \lambda \mathrm{id}) = (g - \lambda \mathrm{id}) g_s'$ i.e. g_s' fixes $V_\lambda := \mathrm{Ker}(g - \lambda)^{\dim V}$ and all eigenvalues of $g_s'|_{V_\lambda}$ are λ as $g - g_s'$ is nilpotent. Hence, as g_s' is semisimple, $g_s' = \lambda \mathrm{id}_{V_\lambda}$. This is also true for g_s. □

Lemma 3.5. *Let $g \in GL(V)$ and $W \subseteq V$ a g-invariant subspace. Then $g_\alpha(W) \subseteq W$ and $g_\alpha|_W = (g|_W)_\alpha$ for any $\alpha \in \{s, n, u\}$.*

Proof. We show that there exist polynomials $P, Q, R \in \Bbbk[T]$ such that $P(0) = Q(0) = R(0) = 0$ and $g_s = P(g)$, $g_n = Q(g)$ and $g_u = R(g)$. From this, invariance of W for g_s, g_n, g_u is clear.

The construction of P is the following: Let $\Phi(T) = \det(T \cdot \mathrm{id}_V - g) = \prod_i (T - \lambda_i)^{n_i}$ be the characteristic polynomial of T. Then

$$\Bbbk[T]/(\Phi) \cong \bigoplus_i \Bbbk[T]/(T - \lambda_i)^{n_i}$$

by the Chinese Remainder theorem. Hence, there is a $P \in \Bbbk[T]$ such that $P \equiv \lambda_i \mod (T-\lambda_i)^{n_i}$ for all i, and $P \equiv 0 \mod T$. Therefore, $P(g) = g_s$. Now, one can define $Q = T - P$ and R can be similarly determined by $g_u = \mathrm{id} + g_s^{-1} g_n$.

By the construction of P, observe that $g_s|_W = P(g)|_W = P(g|_W)$ is semisimple and similarly for the others. □

Terminology: Let V be a (not necessarily finite dimensional) $\Bbbk$-vector space, $g \in GL(V)$. We say that g is semisimple if $g|_W$ is semisimple for all finite dimensional g-invariant subspace $W \subseteq V$. Moreover, we say that g is locally unipotent if $g|_W$ is unipotent for all finite dimensional g-invariant subspace $W \subseteq V$.

Corollary 3.6. *For g and V as above, assume that V is a union of finite dimensional g-invariant subspaces. Then there exist unique elements $g_s, g_u \in GL(V)$ such that g_s is semisimple, g_u is locally unipotent such that $g = g_s g_u = g_u g_s$. Moreover, if $W \subseteq V$ is g-invariant then $g_s|_W = (g|_W)_s$ and $g_u|_W = (g|_W)_u$.*

Proof. We may take the multiplicative Jordan decomposition for each finite dimensional g-invariant subspaces. On the intersections, these are the same by uniqueness of Lemma 3.4 and by preservation of Lemma 3.5, hence we may define it on the linear span of two g-invariant subspaces. This extends to the whole space, by the assumption. □

Let G be an affine algebraic group, $g \in G$ and $\rho_g \in GL(\mathcal{A}_G)$ and $\mathcal{A}_G$ is a union of finite-dimensional vector spaces by Lemma 2.7. Therefore, by Corollary 3.6, there exist unique elements $(\rho_g)_s$ semisimple and $(\rho_g)_u$ locally unipotent such that $\rho_g = (\rho_g)_s(\rho_g)_u = (\rho_g)_u(\rho_g)_s$.

Theorem 3.7. *For any $g \in G$:*

1. *There is a unique decomposition $g_s, g_u \in G$ such that $\rho_{g_s} = (\rho_g)_s$, $\rho_{g_u} = (\rho_g)_u$ and $g = g_s g_u = g_u g_s$.*
2. *For $G = GL_n$ the elements g_s, g_u are the previous ones.*
3. *If $\varphi \hookrightarrow GL_n$ then $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$.*

Lemma 3.8. *Let V be a finite dimensional vector space. Then $g \in GL(V)$ is semisimple if and only if $\rho_g \in GL(\mathcal{A}_{GL(V)})$ is semisimple. Similarly, $g \in GL(V)$ is unipotent if and only if ρ_g is locally unipotent.*

Proof. (Sketch) Recall that $\mathcal{A}_{GL(V)} \cong \Bbbk[x_{11}, \dots, x_{nn}, \det(X)^{-1}]$ if we pick a basis. The element ρ_g acts not just on $\mathcal{A}_{GL(V)}$ but also on $\mathcal{A}_{\mathrm{End}(V)}$. Denote $D := \det(X)$. We claim that $fD^{-m} \in \mathcal{A}_{GL(V)}$ is an eigenvector for ρ_g for all m if and only if $f \in \mathcal{A}_{\mathrm{End}(V)}$ is an eigenvector of ρ_g. Indeed,

$$\rho_g(fD^{-m})(x) = f(xg)D^{-m}(x)D^{-m}(g) = D^{-m}(g)(\rho_g(f)D^{-m})(x)$$

hence ρ_g acts via multiplication of $D^{-m}(g) \in \Bbbk$ if f is an eigenvector, and vice versa. So ρ_g is semisimple on $\mathcal{A}_{GL(V)}$ if and only if it is semisimple on $\mathcal{A}_{\mathrm{End}(V)}$. Similarly, it is locally unipotent on $\mathcal{A}_{GL(V)}$ if and only if it is locally unipotent on $\mathcal{A}_{\mathrm{End}(V)}$. (Its proof is an exercise, use that if ρ_g is locally unipotent then $D(g) = 1$).

Note that $\mathcal{A}_{\mathrm{End}(V)} = \mathrm{Sym}\big(\mathrm{End}(V)^\vee\big) \cong \Bbbk[x_{11}, \dots, x_{nn}]$. As ρ_g acts on $\mathrm{End}(V)^\vee$ by $\rho_g(f)(x) = f(xg)$, it also acts on $\mathrm{Sym}\big(\mathrm{End}(V)^\vee\big)$. We claim that ρ_g is semisimple on $\mathrm{End}(V)^\vee$ if and only if it is semisimple on $\mathrm{Sym}\big(\mathrm{End}(V)^\vee\big)$. Similarly, it is unipotent on $\mathrm{End}(V)^\vee$ if and only if it is locally unipotent on $\mathrm{Sym}\big(\mathrm{End}(V)^\vee\big)$. Indeed, for semisimplicity it is clear, as a diagonal basis of $\mathrm{End}(V)^\vee$ gives a diagonal basis of $\mathrm{Sym}\big(\mathrm{End}(V)^\vee\big)$ and vice versa. The other case is similar.

Finally, note (and prove as an exercise) that g is semisimple on V if and only if it is semisimple on $\mathrm{End}(V)^\vee$ and similarly for unipotence. □

Proof of Theorem 3.7. Take $\varphi : G \hookrightarrow GL(V)$ and the induced map $\mathcal{A}_{GL(V)} \xrightarrow{\varphi^*} \mathcal{A}_G$ such that $\rho_g \circ \varphi^* = \varphi^* \circ \rho_{\varphi(g)}$. For $\varphi(g)$ there exists a unique Jordan decomposition $\varphi(g) = \varphi(g)_s \varphi(g)_u$ in $GL(V)$.

Claim 3.9. $\varphi(g)_s \in \varphi(G)$ and $\varphi(g)_u \in \varphi(G)$

It is enough to prove the claim i.e. that there exist elements $g_s, g_u \in G$ such that $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$. Indeed, then $\varphi(g_s)$ is semisimple, hence $\rho_{\varphi(g_s)} \in GL(\mathcal{A}_{GL(V)})$ is also semisimple by Lemma 3.8, and so is its image ρ_{g_s} under the map $GL(\mathcal{A}_{GL(V)}) \to GL(\mathcal{A}_G)$. Similarly, ρ_{g_u} is locally unipotent, and we got $\rho_g = \rho_{g_s}\rho_{g_u}$ hence $(\rho_g)_s = \rho_{g_s}$ and $(\rho_g)_u = \rho_{g_u}$. Both uniqueness and the independence of g_s and g_u of the choice of the representation $G \hookrightarrow GL(V)$ follow from the uniqueness of the Jordan decomposition, Lemma 3.4.

Proof of the claim. Denote $I := \mathrm{Ker}(\varphi^*)$. If $\tilde{g} \in GL(V)$ then $\tilde{g} \in \varphi(G)$ if and only if $h\tilde{g} \in \varphi(G)$ for all $h \in \varphi(G)$, equivalently if $\rho_{\tilde{g}}(I) \subseteq I$. By the "moreover" part of Corollary 3.6, $(\rho_{\tilde{g}})_s(I) \subseteq I$ and $(\rho_{\tilde{g}})_u(I) \subseteq I$. The claim follows by the above observation. □

□

Third Lecture, 26th of January

Remark 3.10. Recall that an element $g \in G$ of an affine algebraic group is semisimple (resp. unipotent) if and only if for all closed embeddings $\varphi : G \hookrightarrow GL_n$, $\varphi(g)$ is diagonalizable (unipotent). Note, however that the sets of semisimple elements G_s and the set of unipotent elements G_u is not necessarily closed or a subgroup. Still, we have seen that $G = G_sG_u = G_uG_s$.

Theorem 3.11. *Let G be a commutative affine algebraic group. Then G_u and G_s are closed subgroups in G and $G \cong G_s \times G_u$ via the product of the natural embeddings.*

Lemma 3.12. *Let V be a finite dimensional vector space and $S \subseteq GL(V)$ a commutative subset. Then there is a complete flag*

$$\{0\} \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

of S-invariant subspaces. If, moreover, every $s \in S$ is semisimple then there is a basis of V consisting of common eigenvectors of S.

In terms of matrices, this means that we can simultaneously upper-triangulize or diagonalize the elements of S.

Proof. If $S \subseteq \Bbbk \mathrm{Id}_V$ then the statement is clear. Otherwise, let $s \in S$ that has a nontrivial eigenspace $0 \neq V_\lambda \subsetneq V$. Then V_λ is S-invariant as

$$stv = tsv = \lambda tv$$

for any $v \in V_\lambda$ and $t \in S$. Now, use induction on dimension and apply it on V/V_λ and V to obtain the first statement. For the second statement write $V = V_\lambda \oplus W$ where W is the direct sum of other eigenspaces of s. Then W is also S-invariant for the same reason, hence we can again apply induction. □

Proof of Theorem 3.11. Fix an embedding $G \hookrightarrow GL(V)$. Apply Lemma 3.12 to G_s and G_u shows that they are both subgroups since in an appropriate basis elements of G_s are diagonal, diagonal matrices form a subgroup such that all of its elements are semisimple. Similarly, unipotent elements are unipotent matrices in an appropriate basis.

Now, we prove that, in fact, we may choose a common basis of V such that every element of G_s is diagonal and every element of G_u is upper triangular in this basis. By the second part of the lemma, we may write $V = \oplus_\lambda V_\lambda$ where V_λ's are common eigenspaces for G_s. By the commutativity of G, V_λ is G-invariant by

$$sgv = gsv = \lambda gv$$

for all $v \in V_\lambda$ and $s \in G_s$. Hence, we may apply Lemma 3.12 again but for V_λ to obtain a basis of V such that every element of G_u is upper triangular (and every element of G_s is scalar) with respect to this basis.

Taking the union of these bases, we get a basis of the whole space V in which the elements of G_s is diagonal and the elements of G_u are upper triangular.

Then, we get closedness of G_s and G_u by

$$G_s = G \cap D_n \qquad G_u = G \cap U_n$$

where D_n is the set of diagonal matrices and U_n is the set of unipotent matrices with respect to the fixed basis. Indeed, $\supseteq$ is true by definition, and $\subseteq$ is true by the choice of the basis. As G, D_n, U_n are closed subsets (in fact subgroups) of $GL(V)$, we get that G_s and G_u are closed.

This observation also implies that $G = G_s \times G_u$ by $G_s G_u = G$ and $G_s \cap G_u = 1$ by considering Jordan normal form. However, we still need that $G_s \times G_u \to G$, $(s, u) \mapsto su$ is an isomorphism of affine varieties. The inverse map is defined by $g \mapsto (g_s, g_u)$ that is well-defined by the uniqueness of Jordan decomposition, see Theorem 3.4. Moreover, $g \mapsto g_s$ is a morphism as we are just "projecting to diagonal matrices" (see previous paragraphs). Then $g \mapsto g_u = g \cdot g_s^{-1}$ is also a morphism by the axioms of algebraic groups. □

Remark 3.13. A generalization of the theorem also holds for nilpotent algebraic groups.

4 Commutative semisimple groups

If G is a commutative semisimple group (i.e. $G = G_s$) then $G \hookrightarrow D_n \subseteq GL_n$. Note that $D_n \cong \mathbb{G}_m^n$.

Theorem 4.1. *Every commutative semisimple group is isomorphic to* $\mathbb{G}_m^r \times \prod_{i=1}^k \mu_{n_i}$.

Definition 4.2. If $G \cong \mathbb{G}_m^r$ i.e. G is connected (as $\mathbb{G}_m$ is irreducible) semisimple commutative then G is called a torus.

Lemma 4.3. (Dedekind) *Let G be a group and $\Bbbk$ a field. Let $\varphi_1, \dots, \varphi_m : G \to \Bbbk^\times$ be distinct group homomorphisms. Then $\varphi_1, \dots, \varphi_m$ are linearly independent in the $\Bbbk$-vector space of maps $G \to \Bbbk$.*

Proof. Assume that $\sum \lambda_i \varphi_i = 0$ is a nontrivial linear combination of minimal length. Fix $g \in G$ such that $\varphi_1(g) \neq \varphi_{i_0}(g)$ for some i_0. For all $g, h \in G$,

$$\sum \lambda_i \varphi_i(gh) = \sum \lambda_i \varphi_i(g) \varphi_i(h)$$

Then

$$\sum \lambda_i \varphi_i(g) \varphi_i = 0$$

but we also have

$$\sum \lambda_i \varphi_1(g) \varphi_i = 0$$

by multiplying the original linear combination by $\varphi_1(g)$. Then subtracting the last two equations give a nontrivial relation by $\varphi_1(g) \neq \varphi_{i_0}(g)$ that is also shorter as φ_1 falls out. That is a contradiction. □

Definition 4.4. Let G be an affine algebraic group. A character of G is a homomorphism $G \to \mathbb{G}_m$ of algebraic groups. These form an abelian group $\hat{G}$ (not necessarily with a natural algebraic variety structure).

Proposition 4.5. *If G is a commutative semisimple algebraic group then $\hat{G}$ is a finitely generated abelian group. Moreover, it has no elements of order* $\operatorname{char}\Bbbk$ *if* $\operatorname{char}\Bbbk > 0$.

Proof. Recall that $\mathcal{A}_{\mathbb{G}_m} \cong \Bbbk[T, T^{-1}]$ with comultiplication $\Delta(T) = T \otimes T$. It follows that every character $\chi : G \to \mathbb{G}_m$ is determined by the image of T under the induced map $\chi^* : \Bbbk[T, T^{-1}] \to \mathcal{A}_G$. It also has to satisfy

$$\Delta\big(\chi^*(T)\big) = \chi^*(T) \otimes \chi^*(T)$$

so $\chi \mapsto \chi^*(T)$ induces a bijection between $\hat{G}$ and invertible group-like (i.e. that satisfy $\Delta(a) = a \otimes a$) elements of $\mathcal{A}_G$. The lemma implies that invertible group-like elements are $\Bbbk$-linearly independent.

Group-like elements in $\mathcal{A}_{\mathbb{G}_m} = \Bbbk[T, T^{-1}]$ are

$$\{T^m \mid m \in \mathbb{Z}\}$$

by the definition of the comultiplication. These span $\mathcal{A}_{\mathbb{G}_m}$ hence there are no more by independence, see Lemma 4.3.

Now, assume that G is commutative semisimple. Then $G \subseteq \mathbb{G}_m^n$ for some $n \in \mathbb{N}$, hence the induced map

$$\varphi^* : \mathcal{A}_{\mathbb{G}_m^n} \to \mathcal{A}_G$$

is a surjective Hopf-algebra map. Here,

$$\mathcal{A}_{\mathbb{G}_m^n} \cong \otimes_{i=1}^n \mathcal{A}_{\mathbb{G}_m} \cong \Bbbk[T_1, T_1^{-1}, \dots, T_n, T_n^{-1}]$$

Therefore, φ^* sends group-like elements into grop-like elements. One can check that invertible group-like elements of $\mathcal{A}_{\mathbb{G}_m^n}$ are exactly the monomials $T_1^{m_1} \dots T_n^{m_n}$ for any $m_i \in \mathbb{Z}$, $i = 1, \dots, n$ by the same argument as before. Consequently, $\hat{\mathbb{G}}_m^n \cong \mathbb{Z}$ and $\varphi^*(T_1^{m_1} \dots T_n^{m_n})$ are invertible group-like elements in $\mathcal{A}_G$ that generate $\mathcal{A}_G$ by surjectivity, hence this is all. Therefore, $\mathbb{Z}^n \cong \hat{\mathbb{G}}_m^n \twoheadrightarrow \hat{G}$.

If $\operatorname{char}\Bbbk = p > 0$ and $\chi : G \to \mathbb{G}_m$ has order dividing p then $\chi^p(g) = \chi(g)^p = 1$ for all $g \in G$, hence $\chi(g) \in \Bbbk^\times$ is a p-th root of unity hence $\chi(g) = 1$. □

Corollary 4.6. *The contravariant functor extending $G \mapsto \hat{G}$ establishes an anti-equivalence of categories between commutative semisimple groups over $\Bbbk$ and finitely generated abelian groups with torsion that is prime to* $\operatorname{char}\Bbbk$.

The inverse functor is $\mathbb{Z}^r \oplus \bigoplus_{i=1}^k \mathbb{Z}/m_i$ maps to $\mathbb{G}_m^r \times \prod_{i=1}^k \mu_{m_i}$.

Remark 4.7. Assume that $\Bbbk$ is a perfect field and G is an affine algebraic group over $\Bbbk$ (equivalently, take a commutative Hopf algebra over $\Bbbk$). Then G is defined to be a torus over $\Bbbk$ if over $\overline{\Bbbk}$ it becomes isomorphic to $\mathbb{G}_m^n$. Then $\Gamma = \operatorname{Gal}(\Bbbk_s, \Bbbk)$ acts on $\hat{G}$ (or on group-like elements in $\mathcal{A}_G$). Then the theorem is that tori correspond to $\mathbb{Z}^r$ equipped with a Γ-action. Even in rank 1 for $\Bbbk = \mathbb{R}$ where $\Gamma = \mathbb{Z}/2$ can act on $\mathbb{Z}$ two ways: trivially or by interchanging signs. The corresponding two tori are $\mathbb{R}^\times$ and the $\mathbb{R}$-curves $SO_2(\mathbb{R}) = \{x^2 + y^2 = 1\} \subseteq \mathbb{A}_{\mathbb{R}}^2$ with the multiplication of $\mathbb{S}^1$. Similarly, in the case of $\Bbbk = \mathbb{Q}$ one obtains a family of tori $\{x^2 - ay^2 = 1\}$ for all $a \in \mathbb{Q}^\times \backslash (\mathbb{Q}^\times)^2$ corresponding to each quadratic extensions.

Proposition 4.8. *Let* $\operatorname{char}\Bbbk = 0$*. If G is a connected commutative (affine) algebraic group, and* $\dim G = 1$ *then $G \cong \mathbb{G}_m$ or $G \cong \mathbb{G}_a$.*

Remark 4.9. The statement is also true in $\operatorname{char}\Bbbk > 0$ but the proof is a lot harder.

Proof. By Theorem 3.11, $G \cong G_u \times G_s$ hence G is either G_u or G_s by $\dim G = 1$ and connectedness. If $G = \mathbb{G}_s$ then $G \cong \mathbb{G}_m$ by Corollary 4.6. If $G = G_u$ then we know that $G \hookrightarrow U_n$. The group U_n has a filtration $U_n \supseteq N_1 \supseteq \dots \supseteq N_r = \{1\}$ with closed normal subgroups such that $N_i/N_{i+1} \cong \mathbb{G}_a$. (Exercise!) Note that either $G \cap N_i = G$ or $G \cap N_i = \{1\}$. Indeed, by $\dim G = 1$, $G \cap N_i$ is either G or finite. However, in $\operatorname{char}\Bbbk = 0$ a finite unipotent group is trivial as a finite commutative group is always diagonalizable and hence elements cannot have all eigenvalues one. Then

$$G = G \cap N_i \hookrightarrow N_i/N_{i+1} \cong \mathbb{G}_a$$

for the appropriately chosen i. As $\mathbb{G}_a$ has no closed subgroup of dimension one, $G = \mathbb{G}_a$. □

Remark 4.10. An alternative method to prove that proposition is the following: If g is unipotent then in characteristic zero we may consider

$$\log(g) := \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(g-1)^i}{i}$$

As g is unipotent, the sum is in fact finite. In this case, $\log(g)$ is nilpotent. If n is nilpotent then

$$\exp(g) = \sum_{i=0}^{\infty}\frac{n^i}{i!}$$

is a finite sum. Note that $\exp\circ\log = \mathrm{Id}_{G_u}$. Now, fix $g \in G$ unipotent and define $\varphi_g : \mathbb{G}_a \to G$ as $t \mapsto \exp\big(\log(t\cdot g)\big)$ that is a morphism of algebraic groups. By $\dim G = 1$, $\mathrm{Im}\varphi_g$ is a one-dimensional subgroup of G and as we will prove images of morphism of algebraic groups are always closed.

Remark 4.11. We will see that all the connected affine algebraic groups of dimension one are commutative. Moreover, for non-affine algebraic groups, the proposition still survives in some form: (by Riemann-Roch) any algebraic curve is either affine or projective. Therefore, it is enough to understand one dimensional abelian varities and – as it will turn out – these are all elliptic curves.

5 Connected solvable groups

Theorem 5.1. (Lie-Kolchin) *Let V be a finite dimensional $\Bbbk$-vector space, $G \subseteq GL(V)$ be a connected solvable subgroup. Then there exists a complete flag of G-invariant subspaces of V.*

Remark 5.2.

1. We do not assume here that G is closed, but for us that is the interesting case now.
2. The converse is also true, without connectedness of G i.e. if there is such a flag then G is the subgroup of upper triangular matrices that is solvable and a subgroup of a solvable group is solvable.
3. The connectedness assumption is necessary. Counterexample:

$$G = D_2 \cup \{A \in GL_2(\Bbbk) \mid a_{11} = a_{22} = 0\}$$

is a closed subgroup of $GL_2(\Bbbk)$ that is not connected and it is also solvable as it is the extension of D_2 with $\mathbb{Z}/2$. However, clearly there is no basis in which it is diagonal.

Lemma 5.3. *Let G be a topological group. If G is connected then $[G,G]$ is also connected.*

Remark 5.4. If G is not connected, $[G,G]$ may not be closed.

Proof. Consider $\varphi^i : G^{2i} \to G$ defined as

$$(x_1,\ldots,x_i,y_1,\ldots,y_i) \mapsto [x_1,y_1]\ldots[x_i,y_i]$$

If G is connected then $\mathrm{Im}(\varphi^i)$ is connected too. However, $[G,G] = \cup_i\mathrm{Im}(\varphi^i)$ where the images are not disjoint, hence their union is also connected. □

Proof of Theorem 5.1. We use induction on $\dim V$: it is enough to show that the elements of G have a common eigenvector $v \in V$. Indeed, if we prove the assertion then take the image of G in $GL(V/\mathrm{Span}(v))$ that is again connected and apply the induction hypothesis. We may also assume that there is no nontrivial G-invariant subspace in V by the induction.

Now, use (a second) induction on the smallest i such that $G^{(i)} = \{1\}$ where $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$ for $i > 0$ and $G^{(0)} = G$. By the definition of solvability, there is such an i. By Lemma 5.3, $G^{(1)}$ is connected and $\left(G^{(1)}\right)^{(i-1)} = \{1\}$ hence we may apply the second induction on $G^{(1)}$. Hence, the linear span W of common eigenvectors of $G^{(1)}$ in V is nonzero. We claim that $W = V$.

It is enough to prove that W is G-invariant, i.e. for any common eigenvector $v \in V$ of $G^{(1)}$, gv is also a common eigenvector. For any $h \in G^{(1)}$

$$h(gv) = g(g^{-1}hg)v = \lambda gv$$

as $G^{(1)}$ is a normal subgroup hence v is an eigenvector of $g^{-1}hg \in G^{(1)}$. We got $W = V$.

We obtained a basis of V such that the matrix of each $h \in [G, G]$ is diagonal. In particular for fixed $h \in G^{(1)}$, this holds for $g^{-1}hg$ for all $g \in G$. However, $g^{-1}hg$ has the same finite set of eigenvalues, hence conjugation by g may only permute its eigenvalues, i.e. h has finite conjugacy class. For fixed $h \in G^{(1)}$ the map $G \to G$, $g \mapsto g^{-1}hg$ has finite image. This map is continuous, hence by the connectedness of G, this map is constant h. Therefore, $G^{(1)} \subseteq Z(G)$. It means that if V_λ is an eigenspace for $h \in G^{(1)}$ then it is G-invariant by $G^{(1)} \subseteq Z(G)$. However, the only nonzero G-invariant subspace is V, hence the elements of $G^{(1)}$ act by multiplication via a scalar. On the other hand, if $h \in G^{(1)}$ then $\det(h) = 1$ so h has matrix $\omega\mathrm{Id}$ where ω is a $\dim V$-th root of unity. Hence, $G^{(1)}$ is finite, but it is also connected by Lemma 5.3 so $G^{(1)} = \{1\}$, G is connected that has a common eigenvector. □

Corollary 5.5. *If G is connected solvable (affine) algebraic group then G_u is a closed normal subgroup.*

Proof. By Theorem 5.1, G embeds into the group T_n of upper triangular matrices for some $n \in \mathbb{N}$ where $G_u = \mathrm{Ker}(G \hookrightarrow T_n \twoheadrightarrow D_n)$ that is clearly a closed normal subgroup as $\{1\} \subseteq D_n$ is closed. □

Fourth Lecture, 2nd of February

6 Nilpotent groups

Definition 6.1. Denote by $G^i := [G, G^{i-1}]$ and $G^0 = G$ the lower central series of G. A group G is called nilpotent if $G^i = \{1\}$ for some $i > 0$.

Theorem 6.2. (Kolchin) *For every unipotent affine algebraic group $G \subseteq GL(V)$ there is a complete G-invariant flag, in particular it is nilpotent.*

Proof. The in particular part follows from the facts that the existence of a complete G-invariant flag gives an embedding of G into U_n, the group of upper triangular matrices for some $n > 0$. Since U_n is solvable,

For the first statement, we apply induction on $\dim(V)$. It is enough to find a nontrivial G-stable subspace of V, assume there is none, i.e. that V is an irreducible G-representation. By Schur's lemma, $\mathrm{End}_{\Bbbk[G]}(V)$ is a skew field, where each element in $D\backslash\Bbbk$ generates a field extension of $\Bbbk$. By $\mathrm{End}_{\Bbbk[G]}(V) \hookrightarrow \mathrm{End}_{\Bbbk}(V)$, this element is algebraic, hence the extension is finite, so by $\Bbbk = \overline{\Bbbk}$, the extension is trivial and $D = \Bbbk$. By the density theorem, $\Bbbk[G] \to \mathrm{End}_{\Bbbk}(V)$ is surjective.

For any $g \in G \subseteq GL(V)$ we have $\mathrm{Tr}(g) = \dim V = n$ as $g - I$ is nilpotent hence $\mathrm{Tr}(g - I) = 0$. In particular, we get that $\mathrm{Tr}((g-1)h) = 0$ for all $h \in G$. As the linear space of $G \subseteq \mathrm{End}_{\Bbbk}(V)$ is the whole $\mathrm{End}_{\Bbbk}(V)$, we get that $\mathrm{Tr}((g-1)\varphi) = 0$ for all $\varphi \in \mathrm{End}_{\Bbbk}(V)$ and $g \in G$. Hence, $G = \{1\}$ but then V cannot be irreducible if $\dim V > 1$. □

Theorem 6.3. *Let G be a connected nilpotent affine algebraic group. Then G_s and G_u are closed normal subgroups in G and the natural multiplication map $G_s \times G_u \to G$ is an isomorphism, i.e. there is a direct product decomposition.*

Proof. (Sketch) It is enough to prove that $G_s \subseteq Z(G)$. Indeed, then G_s is a commutative semisimple subgroup, hence simultaneously diagonalizable. Embed G into $GL(V)$ faithfully, and let V_λ be a common eigenspace of G_s. It is G-stable hence we may apply Lie-Kolchin Theorem 5.1 to V_λ obtained that $\mathrm{Im}(G) \subseteq GL(V_\lambda)$ has upper triangular form in some basis. By the same procedure, we may find a basis in all the eigenspaces, hence G has upper triangular form in a basis. Then $G_s = G \cap D_n$ is a closed central (hence normal) subgroup, moreover, by Corollary 5.5, G_u is also closed normal. The claim follows.

Assume that $G_s \not\subseteq Z(G)$ and let $g \in G_s$, $h \in G$ such that $[g, h] \neq 1$. Then by Theorem 5.1 there is a complete G-stable flag $V_1 \subseteq \cdots \subseteq V_n = V$. Choose i_0 to be the maximal i such that $g|_{V_i}$ and $h|_{V_i}$ commute but $g|_{V_{i+1}}$ and $h|_{V_{i+1}}$ do not. Write $V_{i+1} = V \oplus \mathrm{Span}\langle v\rangle$ for some $v \in V$. Then necessarily $gh(v) \neq hg(v)$. Now, set $h_1 := [g, h]$, calculation shows that $gh_1(v) \neq h_1g(v)$. Continue by defining $h_i := [g, h_{i-1}]$ for all $i > 0$, we get that $gh_i(v) \neq h_ig(v)$. However, $h_i \in G^i$ so by nilpotent $h_i = 1$ for a sufficiently large i, and that is a contradiction. □

Later:

1. If $\varphi : G \to H$ is a homomorphism of affine algebraic groups then $\mathrm{Im}(\varphi)$ is closed.
2. If $H \lhd G$ is a closed normal subgroup then G/H exists as an affine algebraic group.

As G embeds into T_n, the group of upper triangular matrices where G_u is sent to U_n, we get that G/G_u embeds into $D_n = T_n/U_n$. If G is nilpotent, this surjection splits, i.e. $G \cong G_u \times G/G_u$.

Theorem 6.4. *Let G be a connected solvable affine algebraic group.*

1. *There is a torus $T \subseteq G$ that maps onto G/G_u isomorphically.*
2. *All such T are conjugate in G.*

Definition 6.5. T is called the maximal torus in G.

Reminder:

- G-module: $\mathbb{Z}[G]$-module,
- 1-cocycle: $\varphi : G \to A$ map such that $\varphi(\sigma\tau) = \varphi(\sigma) + \sigma\varphi(\tau)$ for all $\sigma, \tau \in G$, the abelian group of 1-cocycles is denoted as $Z^1(G, A)$,
- 1-coboundary: $\varphi : G \to A$ map such that $\varphi(\sigma) = a - \sigma a$ for some $a \in A$, the abelian group of 1-coboundaries is denoted as $B^1(G, A)$,
- first cohomology: $H^1(G, A) := Z^1(G, A)/B^1(G, a)$

Let E be an extension of G by an abelian group A i.e. $E/A \cong G$, then G acts on A as $(\sigma, a) \mapsto \tilde{\sigma}a\tilde{\sigma}^{-1}$ where $\tilde{\sigma}$ is a lift of σ to E. Given two sections $s_1, s_2 : G \to E$ (i.e. group homomorphisms) to $p : E \to G$ we may construct a 1-cocycle $G \to E$ by taking $\sigma \mapsto s_1(\sigma)s_2(\sigma)^{-1}$ since

$$s_1(\sigma\tau)s_2(\sigma\tau)^{-1} = s_1(\sigma)s_2(\sigma)s_2(\sigma)^{-1}s_1(\tau)s_2(\tau)^{-1}s_2(\sigma)^{-1} = s_1(\sigma)s_2(\sigma)^{-1}\sigma\big(s_1(\tau)s_2(\tau)^{-1}\big)$$

If $\sigma \mapsto s_1(\sigma)s_2(\sigma)^{-1}$ is a 1-coboundary, then by definition there is an $a \in A$ such that $s_1(\sigma)s_2(\sigma)^{-1} = a\sigma(a)^{-1}$ for all $\sigma \in G$. Equivalently, $s_1(\sigma) = as_2(\sigma)a^{-1}$ i.e. the two sections are conjugate. In particular, if $H^1(G, A) = 0$ then any two sections $s_1, s_2 : G \to E$ are conjugate.

Lemma 6.6. *If G is finite of order n then $nH^1(G, A) = 0$.*

Proof. Let $\varphi : G \to A$ be a 1-cocycle and fix $\tau \in G$. Consider $\varphi^\tau : G \to A$ defined as $\sigma \mapsto \varphi(\sigma\tau) - \varphi(\tau)$. One can check that it is a cocycle. In fact,

$$(\varphi^\tau - \varphi)(\sigma) = \varphi(\sigma\tau) - \varphi(\tau) - \varphi(\sigma) = \sigma\varphi(\tau) - \varphi(\tau)$$

where the right hand side is a coboundary, hence $[\varphi] = [\varphi^\tau] \in H^1(G, A)$.

For all $\sigma \in G$ we have

$$\sum_{\tau \in G} \varphi^\tau(\sigma) = \sum_{\tau \in G} \varphi(\sigma\tau) - \sum_{\tau \in G} \varphi(\tau) = 0$$

however, the class of the left hand side in $H^1(G, A)$ is $n \cdot [\varphi]$ and the claim follows. □

Corollary 6.7. *If $|G| = n < \infty$ and A is either a $\mathbb{Q}$-vector space or finite with exponent prime to n then $H^1(G, A) = 0$.*

Lemma 6.8. *Let G be a commutative unipotent affine algebraic group. If $\operatorname{char}\Bbbk = 0$ then G is a $\mathbb{Q}$-vector space. If $\operatorname{char}\Bbbk = p > 0$ then the elements of G have p-power order.*

Proof. By the Lie-Kolchin Theorem 5.1 G embeds into the group of unipotent matrices U_n. The group U_n has a composition series $N_1 \supseteq N_2 \supseteq \dots$ where $N_i/N_{i+1} \cong \mathbb{G}_a$ for all i. If $\operatorname{char}\Bbbk = p > 0$ then the claim follows. Assume that $\operatorname{char}\Bbbk = 0$. Then for all i, either $N_i \cap G = N_{i+1} \cap G$ or $(N_i \cap G)/(N_{i+1} \cap G) \cong \mathbb{G}_a$ indeed, it cannot be finite as a unipotent group is connected in characteristic zero. Observe that $\mathbb{G}_a$ is a $\mathbb{Q}$-vector space, hence G is a successive extension of $\mathbb{Q}$-vector spaces. As G is commutative and $\mathbb{Q}$-vector spaces are injective (as divisible), G is also a $\mathbb{Q}$-vector space. □

Lemma 6.9. *Let G be a connected solvable affine algebraic group and $U \subseteq G$ a closed normal unipotent subgroup. Then the image in G/U of the centralizer Z of a semisimple element $s \in G$ is exactly the centralizer of the image of s in G/U.*

Proof. We reduce to the case when U is commutative by induction on the length of the commutator series of U. Assume that the lemma holds for commutative U, then it holds for smallest nontrivial term $U^{(n)}$ in the series. Then we may apply induction hypothesis on $G/U^{(n)}$ and the claim follows.

Assume that U is commutative and take the Zariski-closure of the generated subgroup of s in G. This is a diagonalizable algebraic group. Indeed, first note that S is a closed commutative subgroup as closure preserves commutativity. Then, by Theorem 3.11, S_s is closed in S and $s \in S_s \subseteq S$ hence $S \subseteq S_s$ also holds by density of the generated subgroup of s. Then, by Theorem 4.1,

$$S \cong \mathbb{G}_m^r \times \prod_{k=1}^{s} \mu_{m_k}$$

for some $m_1, \dots, m_s$. Let n to be prime to $\operatorname{char}\Bbbk$ and let S_n be the n-torsion part of S. By the above description, S_n is a finite subgroup. Moreover,

$$S = \overline{\bigcup_{n \in \mathbb{N}} S_n}$$

again, by the again characterization. Let Z_n be the centralizer of S_n, a closed subgroup in G. Then we have $Z = \cap_{n \in \mathbb{N}} Z_n$ by density. One can check that if the statement holds for S_n instead of s and Z_n instead of Z then by the above density argument, it follows for s and Z.

Let $g \in G$ be such that $g \bmod U$ commutes with $S_n \bmod U$. We have to show that $gu \in Z_n$ for some $u \in U$. We know that for all $\sigma \in S_n$ there is an element $\varphi(\sigma) \in U$ such that $\sigma g \sigma^{-1} = g\varphi(\sigma)$ by the assumption. We claim that $\varphi : S_n \to U$ defined this way is a 1-cocycle, where S_n acts on U by conjugation.

$$\varphi(\sigma\tau) = g^{-1}\sigma\tau g \tau^{-1}\sigma^{-1} = (g^{-1}\sigma g \sigma^{-1})\sigma(g^{-1}\tau g \tau^{-1})\sigma^{-1} =$$

$$= \varphi(\sigma)\sigma\varphi(\tau)\sigma^{-1}$$

but as S_n acts by conjugation, it really proves that φ is a 1-cocycle. By Lemma 6.8, we may apply Corollary 6.7 with $G = S_n$ and $A = U$ as S_n consists of roots of unity. Hence, we get that φ is a coboundary i.e. $\varphi(\sigma) = u(\sigma u \sigma^{-1})^{-1}$ for some $u \in U$ as the action is by conjugation. Expanding the definition of φ, we get

$$\sigma g \sigma^{-1} = gu(\sigma u \sigma^{-1})^{-1}$$

hence $\sigma g u = g u \sigma$ so σ commutes with gu as we claimed. □

Proof of Theorem 6.4. Assume first that every $s \in G_s$ centralizes G_u. If G_u is commutative then G is a central extension of a torus G/G_u with a commutative unipotent group G_u. This means that G is nilpotent, hence by Theorem 6.3, $G \cong G_u \times G/G_u$ hence we found the torus.

If G_u is noncommutative then we apply induction on the length of the commutator series. If G_u^n is the smallest nontrivial term of the series then it is commutative, and by induction, there exists a torus T in G/G_u^n mapping isomorphically on G/G_u. Let $\tilde{T}$ be the preimage of T in G. We know that $\tilde{T}$ is a central extension of T by G_u^n using the assumption that G_s centralizer G_u. Then, again, $\tilde{T}$ is nilpotent hence it is isomorphic to $T \times G_u^n$ by Theorem 6.3 and we are done.

Assume that there is an element $s \in G_s$ that does not centralize G_u, in particular its centralizer is not G. We prove by induction on $\dim G$. Let Z be the centralizer of s in G, this is a closed subgroup in G, in fact it is solvable as G is solvable. Note, however, that Z is not necessarily connected. We know that G/G_u is commutative so we may apply Lemma 6.9 so the image of Z in G/G_u is the whole group. Let Z^0 be the identity component of Z. Since G/G_u is connected, it follows that Z^0 also surjects on G/G_u for dimension reasons. If $\dim Z^0 < \dim G$ then by induction there is a torus $T \subseteq Z^0$ such that T surjects onto $Z^0/Z_u^0 = Z^0/(G_u \cap Z^0)$. The first claim follows.

To prove the second claim, one can check that we may reduce (by induction on the length of the commutator series) to the case when G_u is commutative, the same way as before as before (see notes). Assume that G_u is commutative. We know that if S and T are maximal tori then $G \cong T \ltimes G_u \cong S \ltimes G_u$. Again, we may write $S = \overline{\cup_n S_n}$ as in the proof of Lemma 6.9. For all $n \in \mathbb{N}$ define the closed subset

$$C_n := \{u \in G_u \mid u S_u u^{-1} \subseteq T\}$$

This defines a decreasing chain $C_1 \supseteq C_2 \supseteq \dots$. Define $C_\infty = \cap_n C_n$ that is $\{u \in G_u \mid uSu^{-1} \subseteq T\}$. It is enough to prove that $C_\infty \neq \emptyset$. The chain of C_n's stabilizes by Noetherian property, so it is enough to prove that $C_n \neq \emptyset$ for all n. Let $G_n := S_n G_u = S_n \ltimes G_u$. By construction the tori $T_n = G_n \cap T$ map isomorphically onto $G_n/(G_u \cap G_n)$ hence $G_n = T_n \ltimes G_u$. Let s_n and t_n be the sections $G_n/(G_u \cap G_n)$ corresponding to S_n and T_n. These two sections are conjugate because $H^1(S_n, G_n) = 0$ by Corollary 6.7. □

Fifth Lecture, 9th of February

7 Homogeneous spaces

Reminder: on the notions of (quasi-)projective variety, its homogeneous coordinate ring, the standard affine open covering of $\mathbb{P}^n$ and the local ring $\mathcal{O}_{X,p}$ defined as $(\mathcal{A}_{X^{(i)}})_{p^{(i)}}$ where $X^{(i)} = X \cap D(x_i)$ and $p^{(i)}$ is the "image" of p in $X^{(i)}$ (the definition can be showed to be independent of the choice of i if $p \in D(x_i)$). Moreover, we have recalled the definition of $\mathcal{O}_X(U) := \bigcap_{p \in U} \mathcal{O}_{X,p}$ defined for an irreducible variety X (or by components for general X), and also the definition of morphisms of quasi-projective varieties (as the maps that pull back regular functions). Note that every quasi-projective variety has an open covering by affine varieties.

Proposition 7.1. *Let $\varphi : X \to Y$ be a morphism of irreducible quasi-projective varieties such that $\varphi(X) \subseteq Y$ is Zariski-dense. Then there is a nonempty open subset $U \subseteq X$ such that $\varphi|_U$ is an open mapping.*

Corollary 7.2. *$\varphi(X)$ contains an open set in Y.*

Lemma 7.3. *If Y is an affine variety then the first projection $p_1 : Y \times \mathbb{A}^1 \to Y$ is an open mapping.*

Proof. It is enough to prove that $p_1(D(f)) \subseteq Y$ is open for every basic open set $D(f) \subseteq Y \times \mathbb{A}^1$. We may write

$$f = \sum_{i=0}^{k} f_i t^i \in \mathcal{A}_Y[t] \cong \mathcal{A}_{Y\times\mathbb{A}^1}$$

We claim that $p_1(D(f)) = \cup_i D(f_i)$. Indeed, if $f(p,\alpha) \neq 0$ for some $(p,\alpha) \in Y \times \mathbb{A}^1$ then there is an i such that $f_i(p) \neq 0$ and conversely, if $f_i(p) \neq 0$ for some i then $f(p,\alpha) = \sum_{i=0}^{k} f_i(p)t^i \neq 0$ hence there is an $\alpha \in \mathbb{k}$ such that $f(p,\alpha) \neq 0$. □

Lemma 7.4. *Proposition 7.1 is true in the case where X and Y are affine and $\varphi^* : \mathcal{A}_Y \hookrightarrow \mathcal{A}_X$ induces an isomorphism $\mathcal{A}_X \cong \mathcal{A}_Y[f]$ for some $f \in \mathcal{A}_X$.*

Proof. As X is irreducible, write $\mathbb{k}(X) := \mathrm{Frac}(\mathcal{A}_X)$ and $\mathbb{k}(Y) := \mathrm{Frac}(\mathcal{A}_Y)$. If f is transcendental over $\mathbb{k}(Y)$ then we may apply the previous Lemma 7.3 since $\mathcal{A}_X \cong \mathcal{A}_Y[t] \cong \mathcal{A}_{Y\times\mathbb{A}^1}$. Hence, assume that f is algebraic over $\mathbb{k}(Y)$ and let F be the monic minimal polynomial of f over $\mathbb{k}(Y)$.

Let $a \in \mathcal{A}_Y$ be the common denominator of the coefficients of F. Now, replace Y by the affine open $D(a)$ and similarly, X by the affine open $\varphi^{-1}(D(a))$. This way, we may assume that $a = 1$ i.e. $F \in \mathcal{A}_Y[t]$. Then we get that $\mathcal{A}_X \cong \mathcal{A}_Y[t]/(F)$ since Euclidean division works as F is monic. In particular, we get that $\mathcal{A}_X$ is a free $\mathcal{A}_Y$ -module of rank $\deg(F)$.

It is enough to show that if $f \in \mathcal{A}_X$ then $\varphi(D(f)) \subseteq Y$ is open. Let $\Phi = \sum_{i=0}^{d} f_i t^i$ ($f_d = 1$) be the characteristic polynomial over $\mathcal{A}_Y$ of the multiplication by f on $\mathcal{A}_X$. We show that $\varphi(D(f)) = \cup D(f_i)$. Let $p \in D(f)$ and consider the corresponding ideal $M_p \subseteq \mathcal{A}_X$. By $f \notin M_p$ there is an i such that $f_i \notin (\varphi^*)^{-1}(M_p)$. Indeed, if $\varphi^*(f_i) \in M_p$ for all i then by $\Phi(f) = 0$ we get that $f^d \in M_p$ hence $f \in M_p$ but that is a contradiction.

Conversely, assume that $q \in D(f_i)$ for some i i.e. $M_q \subseteq \mathcal{A}_Y$ such that $f_i \notin M_q$. We claim that $f \notin \sqrt{M_q\mathcal{A}_X}$. It is enough to prove this as the radical of an ideal is the intersection of the maximal ideals containing it hence the claim implies that there is a maximal ideal $M_r \subseteq \mathcal{A}_X$ such that $f \notin M_r \supseteq M_q\mathcal{A}_X$ i.e. that $r \in D(f)$ is a point that maps to $q \in D(f_i)$.

If $f \in \sqrt{M_q\mathcal{A}_X}$ then there is an $m > 0$ such that $f^m \in M_q\mathcal{A}_x$ hence the image $\overline{f}$ of f in

$$\mathcal{A}_X/M_q\mathcal{A}_x \cong (\mathcal{A}_Y/M_q)^d \cong \mathbb{k}^d$$

is a nilpotent endomorphism with characteristic polynomial t^d but that contradicts the fact that $f_i \notin M_p$. □

Proof of Proposition 7.1. Let $U \subseteq Y$ be an affine open and $V \subseteq \varphi^{-1}(U)$ another affine open subset. We may replace X by V and Y by U i.e. we are in the case when X and Y are affine varieties. Then $\mathcal{A}_X$ is a finitely generated $\mathcal{A}_Y$-algebra via $\varphi^* : \mathcal{A}_Y \to \mathcal{A}_X$. Write $\mathcal{A}_X$ as $\mathcal{A}_Y[f_1,\dots,f_r]$ for some $f_i \in \mathcal{A}_X$. Then we may apply Lemma 7.4 on every step of the chain

$$\mathcal{A}_Y \to \mathcal{A}_Y[f_1] \to \cdots \to \mathcal{A}_Y[f_1,\dots,f_r]$$

obtaining the statement. □

Lemma 7.5. *Let Let $\varphi : X \to Y$ be a morphism of irreducible affine varieties. Assume that induces $\mathcal{A}_X \cong \mathcal{A}_Y[f]$, where f is separable over $\mathbb{k}(Y)$. Then there is an open $V \subseteq Y$ such that for all $q \in V$ there is exactly d preimages where $d := [\mathbb{k}(X) : \varphi^*(\mathbb{k}(Y))]$. (See the notes for the proof)*

Corollary 7.6. *Let $\varphi : X \to Y$ be an injective morphism of irreducible quasi-projective varieties with Zariski-dense image. If $\mathbb{k}(X) \mid \varphi^*\mathbb{k}(Y)$ is finite separable then $\mathbb{k}(X) = \varphi^*\mathbb{k}(Y)$.*

Proposition 7.7. *Let $\varphi : G \to G'$ be a morphism of (not necessarily affine) algebraic groups. Then $\varphi(G) \subseteq G'$ is closed.*

Proof. First, assume that G and G' are connected. Let H be the Zariski-closure of $\varphi(G)$ in G'. Then $H \subseteq G'$ is a subgroup. By Corollary 7.2, $\varphi(G)$ contains an open subset U of G'. Then

$$\varphi(G) = \bigcup_{g \in G} \varphi(g)U$$

Hence, $\varphi(G)$ is an open (and dense) subset of H. However, H is irreducible as G is irreducible and the image and closure of an irreducible subset is irreducible. By irreducibility, $h\varphi(G) \cap \varphi(G) \neq \emptyset$ for all $h \in H$ i.e. $h \in \varphi(G)\varphi(G)^{-1} \subseteq \varphi(G)$. The claim follows for this case.

If G is not connected, let G^o be the identity component of G that is a finite index connected subgroup. Then $\varphi(G^o) \subseteq G'$ is closed, hence

$$\varphi(G) = \varphi\Big(\bigcup_{i=1}^{n} g_i G^o\Big) = \bigcup_{i=1}^{n} \varphi(g_i)\varphi(G^o)$$

is also closed. □

Proposition 7.8. *If G is a connected algebraic group then $[G, G]$ is closed and connected.*

Remark 7.9. We have seen that it is connected. Closedness is not necessarily true without the assumption of connectedness.

Proof. Consider the map $\varphi_i : G^{2i} \to G$ defined as

$$(g_1, \dots, g_i, h_1, \dots, h_i) \mapsto [g_1, h_1] \cdot \dots \cdot [g_i, h_i]$$

Then $\{\mathrm{Im}(\varphi_i)\}_{i \in \mathbb{N}^+}$ is an increasing chain of connected (hence, irreducible) subsets with $\cup_i \mathrm{Im}(\varphi_i) = [G, G]$. Let Z_i be the Zariski closure of $\mathrm{Im}(\varphi_i)$. Then $H = \cup_i Z_i = \overline{[G, G]}$ as Z_i is irreducible hence there is an $n \in \mathbb{N}$ such that $Z_n = Z_{n+1} = \cup_i Z_i$ by the finiteness of Krull dimension. We show that $H = [G, G]$.

By Lemma 7.2, there is a nonempty open subset $U \subseteq \mathrm{Im}(\varphi_n) \subseteq H$. By irreducibility of H, for all $h \in H$ we have $U \cap hU \neq \emptyset$. Hence,

$$H \subseteq U \cdot U^{-1} \in \mathrm{Im}(\varphi_n) \cdot \mathrm{Im}(\varphi_n)^{-1} = \mathrm{Im}(\varphi_{2n}) = \mathrm{Im}(\varphi_n) = [G, G]$$

as we claimed. □

Definition 7.10. Let G be an algebraic group and Y a variety. A left action of G on Y is a morphism of varieties $G \times Y \to Y$ that is also an action in the sense of abstract groups.

Remark 7.11. In particular, for all $g \in G$ we may take $\varphi_g : Y \to Y$ that is an isomorphism of varieties.

Proposition 7.12. *Let G be algebraic group acting on a quasi-projective variety Y. Then each orbit of G is open in its closure.*

Example 7.13. It is not necessarily open, e.g. $\mathbb{G}_m$ acting on $\mathbb{A}^1$ by $(\lambda, x) \mapsto \lambda x$ has two orbit, and one is not closed.

Proof. We may assume that g is connected the same way as before. Let $O_p = \{gp \mid g \in G\} = \mathrm{Im}(G \to Y,\ g \mapsto gp)$ be the orbit of $p \in Y$. Let Z be the closure of O_p. By the proposition O_p contains an open subset $U \subseteq Z$. But $O_p = \cup_g gU$ hence $O_p \subseteq Z$ is open. □

Corollary 7.14. (Closed orbit lemma) *If Y is affine or projective, irreducible variety then an orbit of minimal dimension is closed.*

Proof. By the assumptions, O_p is a quasi-projective variety. Let O_p be an orbit of minimal dimension and Z the closure of O_p. Then Z is a union of G-orbits. Indeed, if $q \in Z$ and U_q is an open neighborhood of q containing $p' \in O_p$ then gU_q is an open neighborhood of $gq \in Z$ containing gp'. Hence, $Z \backslash O_p$ does not contain any irreducible component of Z because the irreducible components of Z are the closure of the irreducible components of O_p. It follows that $Z \backslash O_p$ is a union of orbits of strictly smaller dimension. By the assumption, it is possible only if it is empty. □

Definition 7.15. A (left) homogeneous space of G is a quasi-projective variety Y with a G-action $G \times Y \to Y$ that is transitive on points of Y.

Proposition 7.16. *For a homogeneous space Y, the irreducible components agree with connected components and they are all isomorphic as varieties.*

Proof. The same as in the case of $Y = G$, see Proposition 0.3. □

Proposition 7.17. *Let G be an algebraic group, X and Y homogeneous spaces for G and $\varphi : X \to Y$ be a G-equivariant morphism. Then φ is an open mapping.*

Proof. Clearly, φ maps a connected component of X into a connected component of Y. Without loss of generality we may assume that X and Y are connected by passing to the stabilizer of the components in G. By Proposition 7.1 we know that there is an affine open $U \subseteq X$ such that $\varphi|_U$ is an open mapping. Then, similarly, $\varphi|_{gU}$ is also an open mapping as φ_g is a homeomorphism. As $X = \cup_g gU$ we get it is an open mapping. □

Reminder on smoothness: If $X = V(f_1, \ldots, f_r) \subseteq \mathbb{A}^n$ is an affine variety, $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ then T_pX is the zero set of

$$\Big\{ \sum_i (\partial_i f_j)(p)(x_i - a_i) \mid j = 1, \ldots, r \Big\}$$

An important fact about it is the Theorem of Zariski: there is a canonical $\mathbb{k}$-isomorphism $T_pX \cong (M_p/M_p^2)^*$ where M_p is the maximal ideal of $\mathcal{O}_{X,p}$. This gives an intrinsic definition of T_pX, hence we may define the tangent space of a point in a quasi-projective variety this way. We also know that $\dim T_pX \geq \dim X$ for all $p \in X$. A point $p \in X$ is a smooth point if and only if $\dim T_pX = \dim X$ and the variety X is called smooth if all of its points are smooth. Moreover, if X is an irreducible quasi-projective variety then the subset of smooth points is a nonempty open subset of X.

Corollary 7.18. *If X is a homogeneous space of an algebraic group G then X is smooth. In particular, G is smooth.*

Sixth Lecture, 16th of February

Goal: Let G be an affine algebraic group, $H \subseteq G$ a closed subgroup. We would like to define G/H as a quasi-projective variety, and if H is normal then G/H is an affine algebraic group.

Proposition 7.19.

1. *Assume that $H \subseteq G$ is a closed subgroup. Then there exists a homogeneous space (i.e. a quasi-projective variety with an algebraic G-action) such that H is the stabilizer of a point.*

2. *If, moreover, H is a normal subgroup then there exists a homomorphism $\varphi : G \to GL(V)$ for some finite dimensional vector space V such that* $\mathrm{Ker}\varphi = H$.

Corollary 7.20. *In the second case, by Proposition 7.7, the image of φ is closed, hence G/H is endowed with the structure of a linear algebraic group.*

Lemma 7.21. (Chevalley) *There exists a homomorphism of algebraic groups $G \to GL(V)$ such that H is the stabilizer of a 1-dimensional subspace $L \subseteq V$.*

Proof. By Corollary 2.8 we know that there exists an embedding $G \subseteq GL(W)$ such that H is a stabilizer of a subspace $W_H \subseteq W$. Then consider $G \to GL(\Lambda^{\dim W_H} W)$ and define $L := \Lambda^d W_H$. Then H stabilizes L by the definition of W_H. We have to prove the converse, that L is only stabilized by H.

Assume that $g \in G$ stabilizes L. We can choose a basis $e_1, \dots, e_n \in W$ such that $e_1, \dots, e_d$ is a basis of W_H and $e_{m+1}, \dots, e_{m+d}$ is a basis of $g(W_H)$. If $m \neq 0$ then $e_1 \wedge \cdots \wedge e_d$ and $e_{m+1} \wedge \cdots \wedge e_{m+d}$ are linearly independent. However, both are elements of L as g stabilizes L and that is a contradiction. Hence, $m = 0$ so $g(W_H) = W_H$ i.e. $g \in H$. □

Proof of Proposition 7.19. Take $G \to GL(V)$ as in the lemma and $L = \langle v \rangle$ the subspace stabilized by H. Consider the G-orbit of L on $\mathbb{P}(V)$, let it be X. By Proposition 7.12, X is open in its closure, in particular, it is quasi-projective. Then X is the space we have been searching for.

For the second part, consider again a vector space V with a homomorphism $G \to GL(V)$ such that H is the stabilizer of a line L. Let V_H be the span of all common eigenvectors of H in V. Then V_H is G-stable. Indeed, if $w \in V_H$ then

$$hgw = g(g^{-1}hg)w = g\lambda w = \lambda gw$$

hence $gw \in V_H$. Hence, we may assume that $V_H = V$. Decompose V as $\oplus_i V_i$ where V_i is an eigenspace of H. Then let

$$W := \{\lambda \in \mathrm{End}(V) \mid \lambda(V_i) \subseteq V_i \ \forall i\} = \bigoplus_i \mathrm{End}(V_i)$$

and define a G-action on $\mathrm{End}(V)$ as $g\lambda = \varphi(g) \circ \lambda \circ \varphi(g)^{-1}$ where $\varphi : G \to GL(V)$. This preserves V_i for all i. Hence, G acts on W i.e. we get a morphism $\rho : G \to GL(W)$. We need to prove that H is the kernel of ρ. Clearly, $H \subseteq \mathrm{Ker}(\rho)$. Conversely, if $g \in \mathrm{Ker}(\rho)$ then

$$\varphi(g) \in Z(W) = Z\Big(\bigoplus_i \mathrm{End}(V_i)\Big) = Z\Big(\bigoplus_i \mathrm{End}(V_i)\Big) = \bigoplus_i \Bbbk \mathrm{id}_{V_i}$$

by the definition of the action of G on W. In particular, it acts on L by multiplication by scalar multiplication, hence $g \in H$. □

Definition 7.22. Let G be an affine algebraic group, $H \subseteq G$ closed subgroup. Consider pairs (X, ρ), where X is a quasi-projective variety and $\rho : G \to X$ is a morphism constant on the left cosets of H. (X, ρ) is the quotient of G by H if for any (X', ρ') there is a unique morphism $\varphi : X \to X'$ such that $\varphi \circ \rho = \rho'$.

Remark 7.23. If it exists, it is unique up to unique isomorphism.

Lemma 7.24. *Assume that (X, ρ) is a pair as in Definition 7.22, and*

1. *each fibre of $\rho : G \to X$ is a left coset of H, (in particular, it is surjective)*
2. *for all open $U \subseteq X$ the map ρ^* induces an isomorphism*

$$\mathcal{O}(U) \to \mathcal{O}(\rho^{-1}U)^H := \{f \in \mathcal{O}(\rho^{-1}U) \mid f(hp) = f(p) \ \forall h \in H\}$$

3. *and X is a homogeneous space of G and $\rho : G \to X$ is a morphism of homogeneous spaces (i.e. G-equivariant morphism).*

Then (X, ρ) is a quotient of G by H.

Proof. Let (X', ρ') be another pair as in Definition 7.22. For any $p \in X$ choose a $g \in G$ such that $\rho(g) = p$ and set $\varphi(p) := \rho'(g)$. By the first assumption, and the definition of pairs, it is well-defined. We have to show that it is a morphism of projective varieties. First, φ is continuous as ρ' is continuous and ρ is open by Proposition 7.17, using the third assumption. Then the second assumption ensures that it is a morphism of between the appropriate sheaves hence it is a morphism of quasi-projective varieties. □

Lemma 7.25. *Let X be an irreducible quasi-projective variety, $f \in \Bbbk(X)$ and assume that $q \in X$ is a smooth point with $f \notin \mathcal{O}_{X,q}$. Then there is a $p \in X$ such that $\frac{1}{f} \in \mathcal{O}_{X,p}$ and $\frac{1}{f}(p) = 0$.*

Remark 7.26. It is not true if q is not smooth. E.g. on the curve $\{y^2 = x^3\} \subseteq \mathbb{A}^2$ $\frac{y}{x}$ is not regular at $(0,0)$ but $\frac{x}{y} \neq 0$ anywhere. If $\dim X = 1$ then $\mathcal{O}_{X,q}$ is a discrete valuation ring hence if $f \in \Bbbk(X)^\times$ then either f or $\frac{1}{f}$ is regular, hence if $f \notin \mathcal{O}_{X,q}$ then $\frac{1}{f}(q) = 0$. In higher dimension, it is not so simple but the lemma is still true.

Proof. We may assume that X is affine and write $f = \frac{g}{h}$ for some $g, h \in \mathcal{A}_X$. As $\mathcal{O}_{X,q}$ is a regular local ring by assumption, it is known to be a unique factorization domain. In $\mathcal{O}_{X,q}$ we have

$$g = u \cdot \prod_{i=1}^{r} p_i^{a_i} \qquad h = v \cdot \prod_{j=1}^{s} q_j^{b_j}$$

for some units $u, v \in \mathcal{O}_{X,q}$ and irreducibles $p_1, \ldots, p_r, q_1, \ldots, q_s$. We may also assume that $(p_i) \neq (q_j)$ for all i, j. We have to find a $p \in X$ such that $g(p) \neq 0$ but $h(p) = 0$. Assume that there is no such p i.e. $h(p) = 0$ implies $g(p) = 0$. In short, $g \in I(V(h))$. By the Nullstellensatz there is an $n \in \mathbb{N}$ such that $g^n \in (h)$ and that it is a contradiction as we are in a UFD. □

Theorem 7.27. *Let G be an affine algebraic group, $H \subseteq G$ a closed subgroup. Then G/H exists as a quasi-projective variety.. Moreover, it is a homogeneous space of G such that H is the stabilizer of a point.*

Proof. Take (X, ρ) as constructed in the proof of Proposition 7.19. Assumptions 1 and 3 of Lemma 7.24 are clearly satisfied by construction. To verify the second condition, if is enough to prove for all $U \subseteq X$ connected affine open subsets of X. We only have to prove that $\rho^* : \mathcal{O}(U) \to \mathcal{O}(\rho^{-1}(U))^H$ is surjective.

Let $f \in \mathcal{O}(\rho^{-1}(U))$ that is constant on all left cosets of H. Equivalently, (ρ, f) is a morphism $\rho^{-1}(U) \to U \times \mathbb{A}^1$. Let Z be the closure of $\mathrm{Im}(\rho, f) \subseteq U \times \mathbb{A}^1$, in particular, it is an affine variety. By Corollary 7.2, $\mathrm{Im}(\rho, f)$ contains a dense open subset $V \subseteq Z$ (by applying the lemma component-wise). Let $\overline{f}$ be the restriction of $\mathrm{pr}_2 : U \times \mathbb{A}^1 \to \mathbb{A}^1$ to V. We claim that there is a $g \in \mathcal{O}(U)$ such that $p^* g = \overline{f}$ where p is the restriction of $\mathrm{pr}_1 : U \times \mathbb{A}^1 \to U$ to V. It is enough as it implies $f = \overline{f} \circ (\rho, f) = g \circ p \circ (\rho, f) = \rho^* g$.

We know that $p : V \to U$ is injective by its definition and its image is dense. In particular, $\dim V = \dim U$. Then $\Bbbk(V) \mid p^*\Bbbk(U)$ is a finite field extension, and it is in fact separable (We do not prove this part, but it is non-trivial. See the notes). Then by Corollary 7.6, $\Bbbk(V) = p^*\Bbbk(U)$ i.e. $\overline{f} = p^* g$ for some $g \in \Bbbk(U)$. Then we only need to prove that $g \in \mathcal{O}(U)$. If $g \notin \mathcal{O}_{U,p}$ for $p \in U$ then by Lemma 7.25 (using that U is smooth by Corollary 7.18) $\frac{1}{g}$ has a zero on U. Then $\frac{1}{f} = \rho^* \frac{1}{g}$ also has a zero on $\rho^{-1}(U)$ by the surjectivity of ρ. However, that is impossible as $f \in \mathcal{O}(\rho^{-1}(U))$. □

Theorem 7.28. *If, moreover, $H \lhd G$ then G/H is an affine algebraic group.*

Proof. Consider $\rho : G \to GL(V)$, $\mathrm{Ker}\rho = H$ constructed at Proposition 7.19/2. and take $G/H := \mathrm{Im}(\rho)$. It is clearly an affine algebraic group as $\mathrm{Im}(\rho) \subseteq GL(V)$ is closed, and we may use the same argument to see that it is the quotient homogeneous space. □

Corollary 7.29. *$PGL(n) := GL_n/Z(GL_n)$ makes sense as an algebraic group. Similarly, $PSL_n = SL_n/Z(SL_n)$ is an algebraic group.*

Seventh Lecture, 23th of February

8 Geometric quotients

Question: Let G be an affine algebraic group, X an affine variety together with a G-action. Is there a quotient of X by the G-action?

Example 8.1. Generally, it is impossible to have a space of orbits as an algebraic variety. E.g. let $\mathbb{G}_m$ act on $\mathbb{A}^1$ by $(\lambda, x) \mapsto \lambda \cdot x$. Then we have two orbits: a closed one $\{0\}$, and an open one $\mathbb{A}^1 \backslash \{0\}$. The latter cannot be a fiber of a map as it is not closed.

Definition 8.2. (Mumford) Consider pairs (Y, ρ) where Y is a quasi-projecitve variety and $\rho : G \to Y$ is constant on G-orbits. Then (Y, ρ) is a *categorical quotient* of X by G if for all (Y', ρ') as above there is a unique morphism $\varphi : Y \to Y'$ such that $\varphi \circ \rho = \rho'$.

Theorem 8.3. *If G is geometrically reductive then the categorical quotient X/G exists and its points correspond to the closed orbits of G on X.*

Definition 8.4. G is called *geometrically reductive*, if for any finite-dimensional representation $G \to GL(V)$, for all $v \in V^G$ there is a homogeneous G-invariant polynomial $f \in \mathrm{Sym}^d(V^\vee)$ on V such that $f(v) \neq 0$. If $d = 1$ (i.e. f is linear) for all $v \in V^G$ then G is called a *linearly reductive group.*

Remark 8.5.

1. One can show that linear reductivity is equivalent to complete reducibility of all finite dimensional algebraic representations.
2. In $\mathrm{char}\mathbb{k} = p > 0$ one can show that GL_n is geometrically reductive but not linearly reductive. In fact, it is a theorem of Nagata that in positive characteristic the only connected linearly reductive groups are tori.
3. G is geometrically reductive if and only if G is reductive i.e. it has no non-trivial connected unipotent normal subgroup. Direction $\Rightarrow$ is not hard, we will see it later. The converse is easy for characteristic zero, and in positive characteristic it was a conjecture of Mumford for several years, finally solved by Haboush around 1975.

Lemma 8.6. *Let G be a geometrically reductive group.*

1. *If* $\mathrm{char}\mathbb{k} = 0$ *then it is, in fact, linearly reductive.*
2. *If* $\mathrm{char}\mathbb{k} = p$ *then $d = p^r$ for some $r \geq 0$ (where r may depend on the choice of $v \in V^G$).*

Proof. Let $v_0 \in V^G$ and $f \in \mathrm{Sym}^d(V^\vee)$ as in the definition, and for a parameter $\lambda \in \mathbb{k}$ consider the affine linear transformation $v \mapsto \lambda v + v_0$. Then we may decompose

$$f(\lambda v + v_0) = \sum_{i=0}^{d} \lambda^i f_i(v)$$

where f is homogeneous of degree i. We know that f and v_0 are G-invariant, hence $v \mapsto f(\lambda v + v_0)$ is G-invariant. In particular, f_i is G-invariant for all i. By homogenity, we have

$$\sum_{i=0}^{d} \lambda^i f_i(v_0) = f(\lambda v_0 + v_0) = (\lambda + 1)^d f(v_0)$$

On the level of coefficients it means

$$\binom{d}{i} f(v_0) = f_i(v_0)$$

If char$\Bbbk = 0$ we get $f_1(v_0) \neq 0$ as $\binom{d}{1} \neq 0$. If char$\Bbbk = p > 0$ then write $d = p^r s$ where $(p, s) = 1$. As $\binom{d}{p^r} \neq 0$ (elementary computation) we get $f_{p^r}(v_0) \neq 0$. (Note that r may depend on v as it depends on the original choice of f.) ☐

Definition 8.7. An action of a group G on a $\Bbbk$-algebra A is locally finite if every finite-dimensional $\Bbbk$-subspace $V \subseteq A$ is contained in a finite-dimensional G-invariant $\Bbbk$-subspace.

Example 8.8. If G is an affine algebraic group acting on an affine variety X then the induced action of G on $\mathcal{A}_X$ is locally finite. We have seen this when $X = G$ and we act via left translations.

Theorem 8.9. (Hilbert, Nagata) *If G is a geometrically reductive affine algebraic group acting on a finitely generated $\Bbbk$-algebra A such that the action is locally finite then A^G is also a finitely generated $\Bbbk$-algebra.*

Remark 8.10.

1. Without the assumption of geometrical reductivity, A^G is not always finite generated. It was a famous problem of Hilbert solved by Nagata: he gave an example of $\mathbb{G}_a^r$ acting on $\mathbb{A}^n$ such that $\Bbbk[x_1, \dots, x_n]^{\mathbb{G}_a^r}$ is not finitely generated.

2. Popov showed that if A^G is finitely generated for all finitely generated $\Bbbk$-algebra A then G is geometrically reductive. (The proof is based on "lifting" the counterexample of Nagata from $\mathbb{G}_a^r$ to any non geometrically reductive group G.)

Lemma 8.11. *Let A be a $\Bbbk$-algebra, G a geometrically reductive group acting on A such that the action is locally finite. If $I \subseteq A$ is a G-invariant ideal then the natural map $A^G \to (A/I)^G$ induces an integral ring extension $A^G/I^G \hookrightarrow (A/I)^G$.*

Moreover, if G is linearly reductive then $A^G/I^G \hookrightarrow (A/I)^G$ is an equality.

Proof. Let $\overline{a} \in (A/I)^G$ and choose a lift $a \in A$ of $\overline{a}$. As the action is locally finite, the G-orbit of a spans a finite dimensional G-invariant subspace $V \subseteq A$. Hence, for all $\sigma \in G$ we have $\sigma a - a \in V \cap I$. It gives a decomposition

$$V = \Bbbk a \oplus (I \cap V)$$

Let $\lambda \in V^\vee$ such that $\lambda(a) = 1$ and $\lambda|_{I \cap V} = 0$. Observe that λ is G-invariant by

$$\lambda(\sigma a) = \lambda(a) + \lambda(\sigma a - a) = \lambda(a)$$

By the definition of geometrical reductivity applied on the representation $V^\vee$ there is an $f \in \mathrm{Sym}^d(V^{\vee\vee}) \cong \mathrm{Sym}^d(V)$ such that $f(\lambda) = 1$.

Choose a basis $v_1, \dots, v_n$ of V such that $v_1 = a$ and $v_i \in I \cap V$ for all $i > 1$. These are coordinate functions on $V^\vee$ and λ corresponds to $(1, 0, \dots, 0)$ in these coordinates. By $f(\lambda) = 1$, f must be of the form $f = v_1^d + \dots$ Hence, the image of f in A/I is $\overline{a}^d$. By construction $f \in A^G$ hence $\overline{a}^d \in A^G/I^G$ and the "moreover" part follows too. ☐

Corollary 8.12. *Assume moreover that $(A/I)^G$ is a finitely generated $\Bbbk$-algebra. Then A^G/I^G is finitely generated as well.*

Proof. Let $a_1, \dots, a_n$ be the generators of $(A/I)^G$. By the lemma, every a_i satisfies a monic polynomial f_i over A^G/I^G. Let $A_0 \subseteq A^G/I^G$ be a $\Bbbk$-subalgebra generated by the coefficients of $f_1, \dots, f_n$. This is finitely generated hence Noetherian and A^G/I^G is a submodule of the finitely generated A_0-module $(A/I)^G$ (as A_0 was chosen that way), hence A^G/I^G is a finitely generated A_0-module as well. The claim follows. ☐

Corollary 8.13. *Let, moreover, $I_1, I_2 \subseteq A$ be G-invariant ideals. If $a \in (I_1 + I_2)^G$ then there is a $d > 0$ such that $a^d \in I_1^G + I_2^G$. In particular, if $I_1 + I_2 = A$ then there is $f_1 \in I_1^G$ and $f_2 \in I_2^G$ such that $f_1 + f_2 = 1$.*

Proof. Let $a = a_1 + a_2$ where $a_1 \in I_1$ and $a_2 \in I_2$. For any $\sigma \in G$ we have

$$\sigma a_1 - a_1 = -\sigma a_2 + a_2 \in I_1 \cap I_2$$

Let $\overline{A} := A/(I_1 \cap I_2)$ and take $\overline{a}_i$ be the natural image of a_i modulo $I_1 \cap I_2$. By (the proof of) Lemma 8.11 applied on $I_1 \cap I_2 \subseteq A$ there is a $d > 0$ such that $\overline{a}_i^d \in I_i^G/(I_1 \cap I_2)^G$. If $\operatorname{char}\Bbbk = 0$ then by Lemma 8.6 $d = 1$ hence we get $a = a_1 + a_2 \in I_1^G + I_2^G$. If $\operatorname{char}\Bbbk = p > 0$ then $d = p^r$ hence

$$a^{p^r} = (a_1 + a_2)^{p^r} = a_1^{p^r} + a_2^{p^r} \in I_1^G + I_2^G$$

and the claim follows. □

Proof of Theorem 8.9. Step 1: (Principle of Noetherian induction) We claim that it is enough to prove the case when $(A/I)^G$ is finitely generated for all non-trivial G-invariant ideal $I \subseteq A$. Assume that A^G is not finitely generated and consider

$$S = \{J \lhd A \mid J \text{ is } G\text{-invariant, } (A/J)^G \text{ is not finitely generated}\}$$

As $(0) \in S$, S has a maximal element by the Noetherian property. We may replace A by $\overline{A} := A/\overline{J}$ where $\overline{A}$ is not finitely generated but $(\overline{A}/I)^G$ is finitely generated for all ideals $I \subseteq A$.

Step 2: We claim that it is enough to prove the case when A^G contains no zero-divisors. Assume $f \in A^G$ is a zero-divisor, and let

$$I = \operatorname{Ann}(f) = \{a \in A \mid fa = 0\}$$

As fA and I are non-trivial G-invariant ideals, we know that $(A/fA)^G$ and $(A/I)^G$ are finitely generated, by step 1. By Corollary 8.12,

$$\overline{A}_1 = A^G/(fA)^G \qquad \text{and} \qquad \overline{A}_2 = A^G/I^G$$

are finitely generated too. By lifting the generators of $\overline{A}_1$ and $\overline{A}_2$ we may take a finitely generated $\Bbbk$-subalgebra $B \subseteq A^G$ such that B maps surjectively onto $\overline{A}_1$ and $\overline{A}_2$. By Lemma 8.11, $(A/I)^G$ is integral over $\overline{A}_2$, hence over B too. Then $(A/I)^G$ is a finitely generated B-module since $(A/I)^G$ is a finitely generated B-algebra that is integral. Hence, there is a finitely generated B-submodule $\sum_{i=1}^n Bc_i \subseteq A$ mapping onto $(A/I)^G$. We claim that $A^G = B + \sum_{i=1}^n Bfc_i$ and so A^G (as a finitely generated module over the finitely generated $\Bbbk$-algebra B) is a finitely generated $\Bbbk$-algebra.

Indeed, if $\sigma \in G$ then $\sigma c_j = c_j + i_j$ for some $i_j \in I$. However, $I = \operatorname{Ann}(f)$ and $f \in A^G$ hence $fc_j \in A^G$ so we get the part $\supseteq$ of the claim. Conversely, as B surjects onto $\overline{A}_1 = A^G/(fA)^G$, for all $a \in A^G$ there is a $b \in B$ such that $a - b \in A^G$ and $a - b = fc$ for some $c \in A$. We need to prove that $fc \in \sum_{i=1}^n Bfc_i$. As the image of f in A/I is G-invariant and not a zerodivisor by $I = \operatorname{Ann}(f)$, the image of c in A/I is G-invariant. Therefore, there is an element $\sum_{i=1}^n b_i c_i \in \sum_{i=1}^n Bc_i$ such that $c - \sum_{i=1}^n b_i c_i \in I$ hence $fc = \sum_{i=1}^n b_i fc_i$ by $I = \operatorname{Ann}(f)$.

Step 3: We claim that it is enough to prove the case when A is a polynomial ring $\Bbbk[x_1, \ldots, x_n]$ and G preserves the homogeneous components of A. Indeed, assume that $a_1, \ldots, a_n$ generate A over $\Bbbk$. As the action of G is locally finite, there is a finite dimensional $V \subseteq A$ containing $a_1, \ldots, a_n$ that can be assumed to be a $\Bbbk$-basis of V. The action of G on V can be written as

$$\sigma a_i = \sum_j a_{i,j,\sigma} a_j$$

for some $a_{i,j,\sigma} \in \Bbbk$. Consider $S = \Bbbk[x_1, \ldots, x_n]$ and define a G-action on S as

$$\sigma x_i = \sum a_{i,j,\sigma} x_j$$

Define $\varphi : S \to A$ as $x_i \mapsto a_i$ that is a G-equivariant morphism onto A. The kernel $\ker(\varphi) \subseteq S$ is G-invariant. If we prove that S^G is a finitely generated $\Bbbk$-algebra then $C = S^G/\ker(\varphi)^G$ is finitely generated $\Bbbk$-algebra too. We claim that, in this case, A^G is a finitely generated C-module and hence a finitely generated $\Bbbk$-algebra.

First, we may assume that A^G and $C \subseteq A^G$ are integral domains by step 2. We claim that for $K = \mathrm{Frac}(C)$ and $L = \mathrm{Frac}(A^G)$ we have $|L : K| < \infty$. Indeed, it is algebraic as $C \subseteq A^G$ is an integral extension by Lemma 8.11. Moreover, we claim that $L \mid K$ is a finitely generated field extension. If A is an integral domain then it is clear as $\mathrm{Frac}(A)$ is finitely generated over $\Bbbk$ and contains L. If A is not an integral domain then let

$$T = \{\text{non-zerodivisors in } A\}$$

If $M \subseteq A_T$ is a maximal ideal then M consists of zero-divisors so $M \cap A^G = 0$ by step 2. In fact, we have $L = \mathrm{Frac}(A^G) \subseteq A_T/M$ by $A^G \subseteq A_T/M$. Here, $A_T/M = \mathrm{Frac}(A/(A \cap M))$ is a finitely generated field extension, hence L is really finitely generated over K.

Let $\tilde{C}$ be the integral closure of C in L. A non-trivial theorem of commutative algebra states that – as C is a finitely generated algebra – $\tilde{C}$ is a finitely generated C-module. Still, by Lemma 8.11, $A^G \subseteq \tilde{C}$ hence A^G is a submodule of a finitely generated module over a finitely generated (hence Noetherian) $\Bbbk$-algebra.

Step 4: We prove the case when $A = \Bbbk[x_1, \ldots, x_n]$ and G preserves the homogeneous components of A. Let us denote by A_d the space of homogeneous polynomials of degree d and take $A_+ := \oplus_{d>0} A_d$. We claim that $A_+^G = A^G \cap A_+$ is a finitely generated ideal in A^G.

We may assume that $A_+^G \neq 0$ and let $f \in A_+^G$ be a homogeneous element (by the assumption on the action, such an f exists). By step 1, $(A/fA)^G$ is a finitely generated $\Bbbk$-algebra hence $A^G/(fA)^G$ too by Corollary 8.12. As f is not a zero-divisor by step 2 and $f \in A^G$ we have $(fA)^G = fA^G$. So A^G/fA^G is a finitely generated $\Bbbk$-algebra hence the image of A_+^G in it is a finitely generated ideal by the Noetherian property. Then the original A_+^G is also finitely generated as we modded out by just (f).

Let $f_1, \ldots, f_r \in A_+^G$ be generators of the ideal A_+^G such that $f_1 = f$ and f_i is homogeneous for all $i > 0$. Let $d_i := \deg(f_i)$ and take a $d > \max_i d_i$. Then

$$A_d^G = \bigoplus A_{d-d_i}^G f_i$$

as before (by $(fA)^G = fA^G$), so we get that A^G is generated as a $\Bbbk$-algebra by $f_1, \ldots, f_r$ and $A_1^G, \ldots, A_{\max_i d_i}^G$. As $\dim A_r < \infty$ for all r, we get that A^G is a finitely generated algebra. □

Eighth Lecture, 2nd of March

Theorem 8.14. *Let G be a geometrically reductive algebraic group acting on an affine variety X. Then the categorical quotient Y exists as an affine variety and every fiber (of closed points) of the map $X \to Y$ contains a unique closed orbit.*

Proof. By Theorem 8.9, $\mathcal{A}_X^G$ is a finitely generated $\Bbbk$-algebra corresponding to an affine variety Y. Let $\rho : X \to Y$ be the one corresponding to the inclusion $\mathcal{A}_X^G \hookrightarrow \mathcal{A}_X$. Note that ρ is constant on G-orbits as for any maximal ideal $m \lhd A$ and $\sigma \in G$ one has $\sigma(m) \cap \mathcal{A}_X^G = m \cap \mathcal{A}_X^G$.

If Y' is an affine variety then the fact that a morphism $f : X \to Y'$ is constant on G-orbits gives that $\mathcal{A}_{Y'} \to \mathcal{A}_X$ factors through $\mathcal{A}_X^G$. However, we need this property for all varieties, not only affine ones.

Lemma 8.15.

1. *If $Z \subseteq X$ is a G-invariant closed subvariety then $\rho(Z) \subseteq Y$ is also closed.*

2. *If $Z, W \subseteq X$ are G-invariant closed subvarieties such that $Z \cap W = \emptyset$ then $\rho(Z) \cap \rho(W) = \emptyset$.*

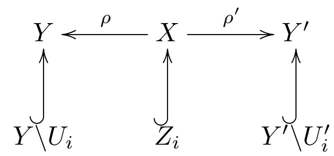
Proof. Let $q \in Y \backslash \rho(Z)$ and take $W := \rho^{-1}(q)$, a closed G-invariant subset. Let I_Z and I_W be the corresponding G-invariant ideals in $\mathcal{A}_X$. By Corollary 8.13 there is an $f \in I_Z^G$ and $g \in I_W^G$ such that $f + g = 1$

by $Z \cap W = \emptyset$. By $f, g \in \mathcal{A}_X^G = \mathcal{A}_Y$ we may consider $f|_{\rho(Z)}$ that is constant zero and $f(q) = 1$ by $g(q) = 0$. Hence, $q \notin \overline{\rho(Z)}$ for any $q \in Y \backslash \rho(Z)$

For the second part, the proof is analogous: For arbitrary G-invariant W, we may take an element $f \in \mathcal{A}_X^G$ such that $f|_{\rho(Z)} = 0$ and $f|_{\rho(W)} = 1$ hence $\rho(Z) \cap \rho(W) = \emptyset$. □

First, we prove that the fibres contain a unique closed orbit. Indeed, first a fibre is a G-invariant set hence it contains a closed orbit as an orbit of minimal dimension is always closed (see Corollary 7.14). Moreover, by the second part of the lemma, the images of two distinct closed orbits are disjoint.

To prove universality, let $\{U_i\}$ be an affine open covering of Y' and define the G-stable open sets $Z_i := X \backslash (\rho')^{-1}(U_i')$. Consider $U_i := Y \backslash \rho(Z_i)$ that are open subsets of Y by the first part of the lemma.



Moreover, by a generalization of the second part of the lemma for $Z_1, \ldots, Z_n$ (that can be proven by straightforward induction), we get that $\cup U_i = Y$. For any basic affine open $D(f) \subseteq U_i$ take $\rho^* f \in \mathcal{O}_X(\rho^{-1} U_i)$ that does not vanish on $X \backslash Z_i$ by $D(f) \subseteq U_i = Y \backslash \rho(Z_i)$. Hence,

$$(\rho|_{X \backslash Z_i})|_{D(\rho^* f)} : D(\rho^* f) \to U_i'$$

is nonzero. The corresponding map $\mathcal{A}_{U_i'} \to \mathcal{A}_{D(\rho^* f)} = (\mathcal{A}_X)_{\rho^* f}$. As ρ' is constant on G-orbits it factors through

$$(\mathcal{A}_X)^G_{\rho^* f} = (\mathcal{A}_X^G)_{\rho^* f} = (\mathcal{A}_Y)_f$$

Hence, we get a map $D(f) \to U_i'$ that is compatible with $\rho'|_{D(\rho^* f)}$. Then, by a gluing argument, one can patch together the morphisms $U_i \to U_i'$ and then to $X \to Y'$. As we had no choice in choosing the morphisms, the result is unique. □

Example 8.16. Let $G = GL_n$ act on $M_n(\Bbbk) = \mathbb{A}_{\Bbbk}^{n^2}$ via conjugation. The categorical quotient (that exists by the theorem modulo the fact that GL_n is geometrically reductive) is given by

$$\rho : M_n(\Bbbk) \to \mathbb{A}^n \qquad A \mapsto (a_{n-1}, \ldots, a_0)$$

where $f_A(t) = \sum_{k=0}^{n} a_k(-t)^k$ is the characteristic polynomial of $A \in M_n(\Bbbk)$. As characteristic polynomial is GL_n-invariant, ρ is constant on orbits. Moreover, we may verify the universal property on it. Let $\rho' : M_n(\Bbbk) \to Y'$ be a morphism that is constant on GL_n-orbits. For any monic polynomial f of degree n let D be a diagonal matrix such that $f_D = f$. Then define $\varphi : \mathbb{A}^n \to Y'$ as $\varphi(f) = \rho'(D)$. Clearly, it is well-defined i.e. independent of the choice of D as diagonal matrices with the same characteristic polynomial are on the same GL_n-orbit and ρ' is constant on orbits.

We have to prove that it is indeed a morphism. We do it only in the case when Y is affine, the general case is a gluing argument. If $f = f_D$ then the coefficients of the characteristic polynomial are the elementary symmetric polynomials of the diagonal entries. As the coordinates of ρ' are given by polynomials that must be symmetric in the entries of D hence by the fundamental theorem of symmetric polynomials, they can be expressed by elementary symmetric polynomials.

In fact, in this case, the closed orbits of $M_n(\Bbbk)$ correspond exactly to the orbits of diagonalizable matrices.

9 Borel fixed point theorem

Theorem 9.1. *Let G be a connected solvable affine algebraic group acting on a projective variety X. Then G has a fixed point.*

Lemma 9.2. *If G is any algebraic group acting on a quasi-projective variety Y then its set of fixed points is closed.*

Proof. It is enough to show that for any $g \in G$, $\{g \in Y \mid gy = y\}$ is a closed set in Y. This set is the inverse image of the diagonal $\Delta(Y) \subseteq Y \times Y$ along the continuous map $Y \ni y \mapsto (y, gy) \in Y \times Y$. □

Proof of Theorem 9.1. We know that $[G, G] \subsetneq G$ is closed and connected by Proposition 7.8. So we may use induction on $\dim G$: assume that $[G, G]$ has a fixed point and let $G/[G, G]$ act on the fixed point set $Y \subseteq X$ that is a G-stable closed subset of X, hence a G-stable projective variety. Then we may assume that G is commutative.

Let Z be a closed orbit in X and $p \in X$ by Corollary 7.14. The stabilizer G_p of p is a closed normal subgroup in G so G/G_p is an algebraic group. In Theorem 7.27 we have seen that $G/G_p \cong Z$ as varieties. However, G/G_p is affine while Z is projective hence $Z = \{p\}$. □

Remark 9.3. Let V be a finite dimensional vector space. Then complete flags $0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ correspond to points of a projective(!) variety $Fl(V)$. This variety is defined as a subvariety of

$$\prod_{k=1}^{n} \mathrm{Gr}_k(V)$$

defined by requiring inclusion of the subspaces. The proof that it is a closed subset is an argument similar to the proof of the existence of $\mathrm{Gr}_k(V)$ as a projective variety.

Definition 9.4. Let G be a linear algebraic group. A subgroup $B \subseteq G$ is a *Borel subgroup* if it is a maximal connected solvable subgroup.

Theorem 9.5. *All Borel subgroups are conjugate.*

Corollary 9.6. *By Theorem 9.5, maximal tori in a connected solvable group are conjugate, so by the previous theorem, they are connected in any linear algebraic group.*

Lemma 9.7. *If $H \subseteq G$ is a closed subgroup such that G/H is a projective variety and B is a Borel subgroup then H contains a conjugate of B.*

Proof. The group $B \subseteq G$ acts on G/H by the left action, hence B has a fixed point by Theorem 9.1, i.e. $BgH = gH$ for some $g \in G$. □

Proof of Theorem 9.5. Fix an embedding $G \hookrightarrow GL(V)$. Then G also acts on the flag variety $Fl(V)$. Let $F \in Fl(V)$ such that its orbit is of minimal dimension hence closed by Corollary 7.14, and in particular a projective variety. Then for $H = G_F$, G/H is isomorphic to the orbit of F as a variety hence by Lemma 9.7, $gBg^{-1} \subseteq H$ for some $g \in G$.

As B is connected, $gBg^{-1} \subseteq H^o$ the identity component of H. However, H^0 is connected and solvable since H is solvable (as the stabilizer of the flag F). By the definition of Borel subgroups, we get $gBg^{-1} = H$. As B was arbitrary, we get that every Borel is conjugate. □

Example 9.8.

1. In GL_n the Borel subgroups are the conjugates of the group of upper triangular matrices.

2. In SL_n the Borel subgroups are the conjugates of the group of unipotent upper triangular matrices, using connectedness

3. (without proof) In SO_n the Borel subgroups are stabilizers of maximal flags $V_1 \subseteq \cdots \subseteq V_r$ such that $\langle ., . \rangle|_{V_i}$ is trivial.

Definition 9.9. Define the *radical* $R(G)$ of G as $\big(\cap_B B\big)^o$ where B runs on the Borel subgroups of B.

Corollary 9.10. *By definition, $R(G)$ is the largest closed connected solvable normal subgroup in G.*

Definition 9.11. An algebraic group G is

- *semisimple* if $R(G) = 0$.
- *reductive* if $R(G)$ is a torus, i.e. the unipotent part $R_u(G)$ of $R(G)$ (called the *unipotent radical*) is trivial.

Example 9.12.

1. SL_n is semisimple, as lower triangular matrices is also a Borel subgroup.
2. GL_n is reductive, by the same trick: the radical is a connected closed subgroup of the diagonal matrices and hence a torus. In fact, the radical of $GL_n = Z(G) = \mathbb{G}_m$.

NINTH LECTURE, 9ND OF MARCH