Mitschrieb: Algebraic Groups
SS 20

Akin

March 11, 2020

Vorwort

Contents

Lecture from 03.03.2020

Recall: Last time we introduced the **Zariski-Topology** on X.
There, algebraic sets equal closed sets.
We called a set X **irreducible** iff each open subset lies dense in X.

Lemma 1. *For an algebraic set X, the following are equivalent:*

(1) X is irreducible.

(2) $k[X] = k[x_1, \dots, x_n]/I(X)$ is a domain.

(3) $I(X)$ is a prime ideal.

The proof of (2) $\iff$ (3) is a basic algebraic result.

Lemma 2. *An open base for the Zariski-Topology on an algebraic set X is given by sets:*

$$D(f) := \{p \in X \mid f(p) \neq 0\}$$

for each $f \in k[X]$. We call the $D(f)$ ***basic open sets****.*

Proof. Suppose $U \subseteq X$ is nonempty and open. Set

$$Z := X \setminus U$$

then Z is closed. Thus

$$Z = \{x \in X \mid f(x) = 0 \forall f \in I\}$$

for some ideal $I \subseteq k[X]$. Let $p \in U$, then there is an $f \in Z$ s.t.

$$f(p) \neq 0.$$

Also, $D(f) \cap Z = 0$, thus $p \in D(f) \subseteq U$. □

Lemma 1. It is clear that (2) is equivalent to (3).
(1) is equivalent to

$$\forall \text{ nonempty, open } U_1, U_2 \subset X : U_1 \cap U_2 \neq \emptyset$$

$$\overset{\text{Lemma 2}}{\iff} \forall \text{ nonempty, basic open } D(f_1), D(f_2) \subset X : D(f_1) \cap D(f_2) \neq \emptyset$$

Since $D(f_1) \cap D_(f_2) = D(f_1 f_2)$, this is equivalent to the statement

$$f_1, f_2 \in k[X] : f_1, f_2 \neq 0 \implies f_1 f_2 \neq 0.$$

Which states that $k[X]$ is a domain. □

Lemma 3. *Let X be an algebraic set. We have bijections*

$$\{\textit{closed subsets } Z \subseteq X\} \leftrightarrow \{\textit{ radical ideals } I \subset k[X]\}$$

and

$$\{\textit{irreducible, closed subsets } Z \subseteq X\} \leftrightarrow \{\textit{ prime ideals } I \subset k[X]\}$$

and

$$\{\textit{points of } X\} \leftrightarrow \{\textit{ maximum ideals } I \subset k[X]\}.$$

Lemma 4 (Primary Decompositions, Atiyah, Macdonald Ch. 4)**.** *For an ideal I we call $P \supseteq I$ a **minimal prime** of I if P is a prime ideal and we have for each prime ideal Q:*

$$P \supseteq Q \supseteq I \implies P = Q.$$

*Any radical ideal I of $k[x_1, \ldots, x_n]$ has only finitely many **minimal** primes $P_1, \ldots, P_r$. Inparticular,*

$$I = \bigcap_{i=1}^{n} P_i$$

and for each i

$$P_j \not\supseteq \bigcap_{j:j\neq i} P_j.$$

Definition 1. An **(irreducible) component** Z of X is a maximal irreducible closed subset, i.e., an irreducible closed $Z \subseteq X$ s.t. there does not exist an irreducible closed $Y \subset X$ s.t. $Y \supsetneq Z$.

Then, we have the bijection

$$\{\text{irreducible components of } X\} \leftrightarrow \{\text{ mimimal primes of } I(X)\}.$$

Lemma 5. *Any algebraic set X has finitely many components $Z_1, \ldots, Z_r$. We have*

$$X = Z_1 \cup \ldots \cup Z_r$$

and for each i

$$Z_i \not\subset \bigcup_{j:j\neq i} Z_j.$$

Example 1.

1. Let $X = V(x \cdot y) \subset k^2$. Then $X = Z_1 \cup Z_2$ where $Z_1 = V(x), Z_2 = V(y)$.

   X is connected, but not irreducible ($D(x)$ does not lie dense in X).

2. Let X be a **finite** algebraic set. It is easy to check that every subset of X is closed:
$$\{p\} = V(x_1 - p_1, \ldots, x_n - p_n)$$
for each $p \in X$. Further
$$X = \{p_1\} \cup \ldots \cup \{p_r\}.$$
Moreover: Any function $f : X \to k$ is regular (i.e. given by polynomials).

Lemma 6. *We call an element $e \in k[X]$* ***idempotent*** *iff $e^2 = e$.*
Let X be an algebraic set. Then
$$\begin{aligned} X \text{ connected} &\iff \text{the only idempotents } e \in k[X] \text{ are 0 and 1} \\ &\iff k[X] \ncong A \times B \text{ for any } k\text{-algebras } A, B. \end{aligned}$$

Lemma 7. *Morphisms of algebraic sets are continuous.*

Proof. Let $\phi : X \to Y$ be a morphism. It suffices to show that for all closed $Z \subset Y$ that $\phi^{-1}(Z) \subset X$ is closed.

But, if
$$Z = V_Y(S) := \{q \in Y \mid f(q) = 0 \forall f \in S\}$$
for some ideal $S \subset k[Y]$, then
$$\phi^{-1}(Z) = V_X(\phi^*(S)) = \{\phi^*(f) = f \circ \phi \mid f \in S\}.$$
□

Lemma 8. *Isomorphisms of algebraic sets are homeorphisms. In particular, any isomorphism of algebraic sets $\phi : X \to X$ permutes the components $Z_1, \ldots, Z_r$ of X:*
$$\forall i \exists j : \phi(Z_i) = Z_j.$$

Theorem 1. *Let G be an algebraic group.*

(i) There is a unique component G^0 of G with $e \in G^0$.

(ii) Every component Z of G is a coset gG^0 of G for some $g \in Z$.

(iii) G^0 is a normal algebraic subgroup of G.

(iv) G^0 is of finite index, i.e.
$$[G : G^0] = \#\left(G/G^0\right) < \infty.$$

(v) *The irreducible components are also the connected components.*

Proof. Let $G = Z_1 \cup \ldots \cup Z_r$ be the decomposition into components. We may assume that $e \in Z_1$.

Recall that $Z_1 \not\subset \bigcup_{j\geq 2} Z_j$. Then, there is an $x \in Z_1 \setminus \bigcup_{j\geq 2} Z_j$. Thus, for all algebraic set isomorphisms $\phi : G \to G$, we have by some previous lemma that $\phi(x)$ is likewise contained in some unique component of G. For example, we may take ϕ to be

$$\begin{aligned} \phi_g : G &\to G \\ y &\longmapsto gy \end{aligned}$$

for any $g \in G$. Then, for all $g \in G$, the element $gx = \phi_g(x)$ is contained in only one component of G. Ergo, each $g \in G$ is contained in exactly one component.

(i) Take $g = e$.

(iii) G^0 is an algebraic subset, by construction. Denote by $m : G \times G \to G$ and $i : G \to G$ the continuous multiplication and inversion map on G. **Why is G^0 a subgroup?** We need to show

$$\begin{aligned} m(G^0 \times G^0) &\subseteq G^0. \\ i(G^0) &\subseteq G^0. \end{aligned}$$

We know that $i(G^0)$ is some component of G, since i is an isomorphism. But it contains the identity e, since $e^{-1} = e$. Therefore, $i(G^0) = G^0$.

If $g \in G$, then gG^0 is some component of G. Suppose $g \in G^0$. Then $gG^0 \cap G^0 \supseteq \{g\}$, therefore $gG^0 = G^0$. Ergo, G^0 is closed under multiplication.

Why is G^0 a normal? If $g \in G$, then gG^0g^{-1} is a component that contains e, therefore $G^0 = gG^0g^{-1}$.

(Alternative proof that $m(G^0 \times G^0) = G^0$: Consider

- any continuous image of an irreducible set is irreducible.
- the closure of any irreducible set is irreducible.

Ergo $\overline{m(G^0 \times G^0)}$ is a closed irreducible set containing e. Ergo, $\overline{m(G^0 \times G^0)} = G^0$).

(ii) Let $Z \subset G$ be a component. Let $g \in Z$. Then $g \in (gG^0 \cap Z)$, so $gG^0 = Z$.

(iv) This follows from some previous lemma.

(v) This is left as a topological exercise. It is true whenever the irreducible components do not intersect.

□

It now follows:

$$\{\text{finite algebraic groups}\} \longleftrightarrow \{finitegroups\}$$

where the above arrow is an equivalence of categories.

Example 2.

- Let $G = \{g_1, \dots, g_r\}$ be a finite algebraic group. Then,
$$G^0 = \{e\}.$$
- Without proofs:
$$G \in \{\mathsf{GL}_n(k), \mathsf{SO}_n(k), \mathsf{SL}_n(k)\} \implies G^0 = G.$$
Further,
$$G = O_n(k) \implies G^0 = \mathsf{SO}_n(k)$$
(but only if $-1 = 1$ i.e. $\mathsf{char}k = 2$. Otherwise $[G : G^0] = 2$.)

0.1 Jordan Decomposition

As usual, $k = \overline{k}$ is an algebraically closed field.

Definition 2. Let V be a finite-dimensional vector space.

An element $x \in \mathsf{End}(V)$ is **semisimple**, if it is diagonalizable, i.e. it has a basis of eigenvectors, or equivalently, if the minimal polynomial of x is square-free.

Then, there is a decomposition $V = \bigoplus_{i=1}^r V_i$ and distinct elements $\lambda_1, \dots, \lambda_n \in k$ s.t.

$$x|_{V_i} = \lambda_i.$$

If $\dim(V_i) = n_i$, then

$$\text{char polynomial of } x = \prod_{i=1}^{r} (T_i - \lambda_i)_i^n \in k[T]$$

and

$$\text{minimal polynomial of } x = \prod_{i=1}^{r}(T_i - \lambda_i) \in k[T].$$

(Where the minimal polynomial of x is defined as the least degree monic m s.t. $m(x) = 0$ and Cayley-Hamilton $m|c$.)

Definition 3. $x \in End(V)$ is **nilpotent** if $x^n = 0$ for some n. (Equivalent to: characteristic polynomial of x is $T^{\dim(V)}$.)

x is **unipotent**, if $x - 1$ is nilpotent.

Lemma 9. *If x is semisimple and nilpotent, then $x = 0$.*

If x is semisimple and unipotent, then $x = 1$.

Lemma 10. *If x, y are commuting elements, thar are semisimple resp. unipotent or nilpotent, then so is xy.*

Theorem 2 (Goal)**.** *For all algebraic groups G and for all $g \in G$, there exist unique group elements $g_s, g_u \in G$ s.t.*

$$g = g_s g_u = g_u g_s$$

and for all finite-dimensional representations $\rho : G \to \mathsf{GL}(V)$, $\rho(g_s)$ is semisimple and $\rho(g_u)$ is unipotent.

Example 3. If $g = \begin{pmatrix} \lambda & 1 & 0 \\ & \lambda & 1 \\ & & \lambda \end{pmatrix} \in G = \mathsf{GL}_3(k)$, then $g_s = \begin{pmatrix} \lambda & 0 & 0 \\ & \lambda & 0 \\ & & \lambda \end{pmatrix}$, $g_u = \begin{pmatrix} 1 & \lambda^{-1} & 0 \\ & 1 & \lambda^{-1} \\ & & 1 \end{pmatrix}$.

Lecture from 09.03.2020

Theorem 3 (Goal Theorem). *Let G an algebraic group. For all $g \in G$ there is exactly one pair $g_s, g_u \in G$ s.t.*

$$g = g_s g_u = g_u g_s$$

and for all finite-dimensional representations $r : G \to \mathsf{GL}_n(V)$, the element $r(g_s)$ resp. $r(g_u)$ is semisimple resp. unipotent.

Last time, we saw:

Lemma 11.
- *If g, h are commuting and semisimple resp. commuting and unipotent then so is gh.*
- *If g is semisimple and unipotent, then $g = 1$.*

Proposition 1. *Let V be a finite-dimensional vector space and $g \in \mathsf{GL}(V)$. There exist unique elements $g_s, g_u \in \mathsf{GL}(V)$ s.t.*

$$g = g_s g_u = g_u g_s$$

and g_s is semisimple and g_u is unipotent.

Moreover, $g_s, g_u \in k[g] = \{\sum_{i=1}^m a_i g^i \mid a_i \in k\} \subseteq \mathsf{End}(V)$.

Proof. **Existence** (Sketch): Say

$$g = \begin{pmatrix} \lambda & 1 & 0 \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}$$

then take

$$g_s = \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix}, \quad g_u = \begin{pmatrix} 1 & \lambda^{-1} & 0 \\ & 1 & \lambda^{-1} \\ & & 1 \end{pmatrix}.$$

For $\lambda \in k$, define the **generalized λ-eigenspace** of g by

$$V_\lambda := \{v \in V \mid \exists n \in \mathbb{N}_0 : \ (g - \lambda)^n v = 0\}.$$

Then

$$V = \bigoplus_{\lambda \in k} V_\lambda.$$

Here V_λ = sum of domains of all Jordan blocks with λs on the diagonal. (It follows from the Jordan Decomposition for matrices that such a decomposition exist.)

Let's define $g_s \in \mathsf{GL}(V)$ by

$$g_s|_{V_\lambda} = \lambda \cdot \mathrm{Id}.$$

Note that $gV_\lambda \subset V_\lambda$, hence g commutes with g_s, hence g, g_s commutes with $g_u := gg_s^{-1}$. Then, $g = g_s g_u = g_u g_s$.

Write $\det(T - g) = \prod_\lambda (T - \lambda)^{n(\lambda)}$, $n(\lambda) = \dim(V_\lambda)$. Since the polynomials $T - \lambda$ for $\lambda \in k$ are coprime, the chinese remainder theorem implies that there is a $Q \in k[T]$ s.t.

$$Q \equiv \lambda \mod (T - \lambda)^{n(\lambda)}$$

for each $\lambda \in k$.

We claim that

$$Q(g) = g_s.$$

Indeed, since $gV_\lambda \subseteq V_\lambda$, we have

$$Q(g)V_\lambda \subseteq V_\lambda.$$

So, it suffices to show for all $v \in V_\lambda$

$$Q(g)v = g_s v = \lambda v.$$

Note that, by Cayley-Hamilton,

$$V_\lambda = \left\{ v \in V \mid (g - \lambda)^{n(\lambda)} v = 0. \right\}$$

Write

$$Q = \lambda + R \cdot (T - \lambda)^{n(\lambda)}$$

for some $R \in k[T]$. Since $(g - \lambda)^{n(\lambda)} v = 0$, deduce that $Q(g)v = \lambda v$, as required.

If $Q' \equiv T(T - \lambda)^{n(\lambda)}$, then

$$Q'(g) = g_u.$$

If $Q'' \equiv \lambda^{-1}(T - \lambda)^{n(\lambda)}$, then $Q''(g) = g_s^{-1}$. check corresponding stuff for g_u.

Uniqueness: Suppose given some other decomposition

$$g = g'_s g'_u = g'_u g'_s$$

with g'_s semisimple and g'_u unipotent. Then g'_s commutes with g'_s and g'_u, hence with g, hence also with any element in $k[g]$. Ergo, g'_s commutes with g_s and g_u. Similarly, g'_u commutes with g_s and g_u.

Consider

$$h := g'_s g_s^{-1} = g'_s g'_u (g'_u)^{-1} g_s^{-1} = g (g'_u)^{-1} g_s^{-1} = g_u (g'_u)^{-1}.$$

Then $h = g'_s g_s^{-1}$ is a product of semisimple elements and $h = g_u(g'_u)^{-1}$ is a product of unipotent elements. By proceeding lemmas, h is semisimple and unipotent, ergo trivial. It follows $g'_s = g_s$ and $g'_u = g_u$. □

Corollary 1. *Let $g \in \mathsf{GL}(V)$, let $W \subset V$ be any g-**invariant subspace**, i.e. $gW \subseteq W$.*

Then, W is g_s-invariant and g_u-invariant.

Proof. This is clear, since g_s and g_u are algebraically generated by g over g. □

Lemma 12. *Let $\phi : V \to W$ be a linear map between finite-dimensional vector spaces.*

Let $\alpha \in \mathsf{GL}(W)$ and $\beta \in \mathsf{GL}(W)$ s.t.

$$\begin{tikzcd} V \arrow[r, "\alpha"] \arrow[d, "\phi"] & V \arrow[d, "\phi"] \\ W \arrow[r, "\beta"] & W, \end{tikzcd}$$

i.e. $\phi \circ \alpha = \beta \circ \phi$.

Then,

$$\phi \circ \alpha_s = \beta_s \circ \phi,$$
$$\phi \circ \alpha_u = \beta_u \circ \phi.$$

Proof. Write $V = \bigoplus_{\lambda \in k} V_\lambda$, $W = \bigoplus_{\lambda \in k} W_\lambda$ where V_λ are the generalized α-eigenspaces and W_λ are the generalized β-eigenspaces.

We claim that

$$\phi(V_\lambda) \subset W_\lambda.$$

Indeed, let $v \in V_\lambda$, then

$$(\beta - \lambda)^n \phi(v) = \phi((\alpha - \lambda)^n v) = 0.$$

Since $(\alpha - \lambda)^n v = 0$, the claim follows.

Since, $\alpha_s|_{V_\lambda} = \lambda \mathrm{Id}$ and $\beta_s|_{W_\lambda} = \lambda \mathrm{Id}$, deduce that

$$\phi \circ \alpha_s = \beta_s \circ \phi.$$

Indeed, both sides are given on V_λ by $\lambda \cdot \phi$. Thus

$$\begin{aligned} \phi \circ \alpha_u &= \phi \circ \alpha\alpha_s^{-1} \\ &= \beta\beta_s^{-1} \circ \phi \\ &= \beta_u \circ \phi. \end{aligned}$$

□

Lemma 13. *Let $\alpha \in \mathit{GL}(V)$, $\beta \in \mathit{GL}(W)$. Then the **tensor** $\alpha \otimes \beta \in \mathit{GL}(V \otimes W)$ is defined by*

$$(\alpha \otimes \beta)(u \otimes v) = \alpha(u) \otimes \beta(v).$$

Then, we have

$$(\alpha \otimes \beta)_s \overset{(1)}{=} \alpha_s \otimes \beta_s$$

$$(\alpha \otimes \beta)_u \overset{(2)}{=} \alpha_u \otimes \beta_u.$$

Proof. It suffices to prove (1), since

$$\begin{aligned} (\alpha \otimes \beta)_u &= (\alpha \otimes \beta) \circ (\alpha \otimes \beta)_s^{-1} \\ &\overset{(1)}{=} (\alpha \otimes \beta) \circ (\alpha_s \otimes \beta_s)^{-1} \\ &= \alpha\alpha_s^{-1} \otimes \beta\beta_s^{-1} \\ &= \alpha_u^{-1} \otimes \beta_u^{-1} \end{aligned}$$

For (1), consider

$$V = \bigoplus_{\lambda \in k} V_\lambda,$$

$$W = \bigoplus_{\lambda \in k} W_\lambda.$$

It follows

$$V \otimes W = \bigoplus_{\lambda, \mu \in k} V_\lambda \otimes W_\mu.$$

Now,

$$\alpha_s \otimes \beta_s|_{V_\lambda \otimes W_\mu} = \lambda\mu \cdot \mathrm{Id}.$$

Ergo, $\alpha_s \otimes \beta_s$ is semisimple. By Proposition, we reduce to checking that $\alpha_u \otimes \beta_u$ is unipotent. Indeed,

$$\alpha_u \otimes \beta_u - 1 = (\alpha_u - 1) \otimes (\beta_u - 1) + 1 \otimes (\beta_u - 1) + (\alpha_u - 1) \otimes 1$$

is nilpotent (You can also check that $\alpha_u \otimes \beta_u = (\alpha_u \otimes 1) \circ (1 \otimes \beta_u)$ is unipotent.) □

Example 4. Let $1 \in \mathsf{GL}(V)$. Then $1_s = 1$ and $1_u = 1$.

Summary : Let G be an algebraic group. Let $r_V : G \to \mathsf{GL}(V)$ be a finite-dimensional representation. Also, fix $g \in G$.

Let $\lambda_V := r_V(g)_s$ (or $r_V(g)_u$).

We get a family of operators $\lambda_V \in \mathsf{End}(V)$ with the following properties:

(i) if $V = k$ and $r_V(g') = 1$ for all $g' \in G$, then $\lambda_V = 1$.

(ii) for any two representations in V and W, we have

$$\lambda_{V\otimes W} = \lambda_V \otimes \lambda_W.$$

(iii) for all G-equivariant $\phi : V \to W$ we have

$$\phi \circ \lambda_V = \lambda_W \circ \phi.$$

Theorem 4. *Let G be an algebraic group. Let $\lambda_V \in \mathsf{End}(V)$ (i.e. $V = (r_V, V)$ is a finite-dim. representation of G) be a family of operations satisfying (i), (ii), (iii).*

Then, there is exactly one $g \in G$ s.t. $\lambda_V = r_V(g)$ for all V.

Note, that this theorem implies our goal theorem.

Applying the theorem to $\lambda_V = r_V(g_s)$ implies

$$\exists g_s \in G : r_V(g_s) = r_V(g)_s$$

and

$$\exists g_u \in G : r_V(g_u) = r_V(g)_u.$$

Proof of Goal Theorem. There exist unique $g_s, g_u \in G$ s.t.

$$g \overset{(*)}{=} g_u g_s = g_s g_u,$$

Then, $r_V(g) = r_V(g_s) r_V(g_u) = r_V(g_u) r_V(g_s)$.

Since $r_V(g_u)$ is unipotent and $r_V(g_s)$ is semisimple, it follows $r_V(g_u) = r_V(g)_u$ and $r_V(g_s) = r_V(g)_s$.

To deduce $(*)$, take any $r_V : G \hookrightarrow \mathsf{GL}(V)$. We know for each V

$$r_V(g) = r_V(g_s) r_V(g_u) = r_V(g_u) r_V(g_s).$$

∎

Proof of Theorem. We first extend the assignment

$$V \mapsto \lambda_V$$

to all representations of G.

Say $V = \bigcup_j W_j$ where each W_j is a finite-dimensional G-invariant subspace. Try to define $\lambda_V \in \mathsf{End}(V)$ by

$$\lambda_V|_{W_j} := \lambda_{W_j}.$$

For this to be well-defined, we need to show for each i, j

$$\lambda_{W_i}|_{W_i \cap W_j} \overset{(*)}{=} \lambda_{W_j}|_{W_i \cap W_j}.$$

Proof of $(*)$**:** Apply assumption (iii) to the G-equivariant linear maps

$$W_i \cap W_j \overset{\phi}{\hookrightarrow} W_i,$$
$$W_i \cap W_j \overset{\phi'}{\hookrightarrow} W_j.$$

Then,

$$\begin{aligned} \lambda_{W_i}|_{W_i \cap W_j} &= \lambda_{W_i} \circ \phi \\ &\overset{(iii)}{=} \phi \circ \lambda_{W_i \cap W_j} \\ &= \phi' \circ \lambda_{W_i \cap W_j} \end{aligned}$$

and

$$\lambda_{W_j}|_{W_i \cap W_j} = \lambda_{W_i} \circ \phi' = \phi' \circ \lambda_{W_i \cap W_j}.$$

Recall here that any finite-dimensional G-invariant $W \subset V$ is a representation. $\square$

[0]Not necessarily finite-dimensional, but may be written as a filtered union of finite-dimensional G-invariant subspaces of W.

Lecture from 11.03.2020

Let G be an algebraic group.

Easy Exercise : If V_1, V_2 are representations r_1, r_2 of G, then $V_1 \otimes V_2$ is also a representation with

$$r = r_1 \otimes r_2 : G \to \mathsf{GL}(V_1 \otimes V_2)$$

given by

$$r(g)(v_1 \otimes v_2) = (r_1(g)v_1) \otimes (r_2(g)v_2).$$

Proof. Given $\Delta_j : V_j \to V_j \otimes k[G]$, define

$$\Delta : V_1 \otimes V_2 \longrightarrow V_1 \otimes V_2 \otimes k[G]$$

by: if

$$\Delta_1 u = \sum u_i \otimes f_i, \quad \Delta_2 v = \sum v_j \otimes h_j,$$

then

$$\Delta(u \otimes v) \sum \sum u_i \otimes v_j \otimes f_i h_j.$$

Set $A := k[G]$, then

$$r_A := \text{right regular representation with } r_A(g)f(x) = f(xg).$$

The map

$$\begin{aligned} A \otimes A &\xrightarrow{m} A \\ f_1 \otimes f_2 &\longmapsto f_1 f_2 \end{aligned}$$

defines a morphism of representations

$$(A, r_A) \otimes (A, r_A) \to (A, r_A).$$

Indeed,

$$\begin{aligned} m((r_A \otimes r_A)(g)(f_1 \otimes f_2))(x) &= f_1(xg)f_2(xg), \\ &= f_1 f_2(xg) = r_A(g)(m(f_1 \otimes f_2))(x), \end{aligned}$$

since $f_1(\_g) \otimes f_2(\_g) = (r_A \otimes r_A)(g)(f_1 \otimes f_2)$.

Ergo $m \circ (r_A \otimes r_A)(g) = r_A(g) \circ m$. □

Recall: We stated the following theorem

Theorem 5. *Let $\lambda_V \in \mathsf{End}(V)$ be given s.t. for all finite-dim. rep.s V of G s.t.:*

(i) $\lambda_k = 1$

(ii) $\lambda_{V\otimes W} = \lambda_V \otimes \lambda_W$

(iii) for all morphisms of rep.s $\phi : V \to W$ we have

$$\phi \circ \lambda_V = \lambda_W \circ \phi.$$

Then, there is exactly one $g \in G$ s.t. $\lambda_V = r_V(g)$ for all V.

Proof. Last time, we saw that any such family $V \mapsto \lambda_V$ extends to **all** rep.s V of G.

Let's note also that, if (V_0, r_0) is any representation of G with trivial action, i.e. $r(g) = 1$ for all g, then $\lambda_{V_0} = 1$. Indeed, let $v \in V_0$. We must check that $\lambda_{V_0} v = v$. Since the action is trivial, any subsapce of V_0 is G-invariant.

Consider the map

$$\begin{aligned} \phi : k &\longrightarrow V_0 \\ \alpha &\longmapsto \alpha v \end{aligned}$$

where $v = \phi(1)$. Then, ϕ is a morphism of rep.s because the action is trivial.

Thus,

$$\lambda_V v = (\lambda_V \circ \phi)(1) \overset{(iii)}{=} (\phi \circ \lambda_k)(1) \overset{(i)}{=} \phi(1) = v.$$

Consider $\lambda_A \in \mathsf{End}(A)$. Then,

$$\lambda_{A\otimes A} = \lambda_A \otimes \lambda_A.$$

It is an easy exercise to see that $m : (A, r_A) \otimes (A, r_A) \to (A, r_A)$ is a morphism of rep.s.

By (iii) it follows, $m \circ (\lambda_A \otimes \lambda_A) = \lambda_A \circ m$, i.e.

$$\lambda_A(f_1 f_2) = \lambda_A(f_1)\lambda_A(f_2)$$

for all $f_1, f_2 \in A$. Thus, λ_A is an algebra morhism (check, using the morphism $k \hookrightarrow A$, that $\lambda_A(1) = 1$).

Thus, $\lambda_A = \phi^*$ for some unique morphism ϕ of algebraic sets $\phi : G \to G$.

We claim that ϕ commutes left multiplication i.e.

$$\phi(hx) = h\phi(x)$$

for all $h, x \in G$. Indeed, let's consider the map

$$\begin{aligned} A &\longrightarrow A \\ f &\longmapsto f(h \cdot \_). \end{aligned}$$

This induces a morphism

$$(A, r_A) \xrightarrow{\psi} (A, r_A).$$

By (ii), $\psi \circ \lambda_A = \lambda_A \circ \psi$.

Since $\lambda_A = \phi^*$, this implies the claim.

Now, set $g := \phi(e)$. Then for all $h \in G$,

$$\phi(h) = \phi(he) = hg.$$

Thus, $\lambda_A = \phi^* = r_A(g)$.

(It remains to show that

$$\lambda_V = r_V(g)$$

for each finite-dim. rep. V.)

Let $V = (V, r)$ be any rep. This induces a map

$$\Delta : V \longrightarrow V \otimes A.$$

If $\Delta v = \sum v_i \otimes f_i$, then

$$hv = \sum f_i(h_i) \otimes v_i.$$

Let

$$\begin{aligned} \varepsilon : V \otimes A &\longrightarrow V \\ v \otimes f &\longmapsto f(1)v. \end{aligned}$$

It follows $\varepsilon \circ \Delta : V \to V$ is the identity map.

Let (V_0, r_0) be the representation of G with $V_0 := V$ and r_0 the trivial action. Then, $\Delta : V \to V_0 \otimes A$ is a morphism of representations.

(Indeed, if $\Delta v = \sum v_i \otimes f_i$, then

$$\Delta(r(h)v) \stackrel{?}{=} (r_0(h) \otimes r_A(h))\Delta v$$

since

$$\begin{aligned} \Delta v &= \sum v_i \otimes f_i \\ \iff xv &= \sum f_i(x_i) v_i \ \forall x \in G \\ \iff xhv &= \sum f_i(xh) v_i \ \forall x, h \in G. \end{aligned}$$

Since $r(h)v = hv$, it follows

$$\Delta(hv) = \sum v_i \otimes f_i(\cdot h) \implies (?).)$$

We want to show

$$\lambda_V = r_V(g).$$

We have

$$\begin{aligned} \Delta \circ \lambda_V &\overset{(iii)}{=} \lambda_{V_0 \otimes A} \circ \Delta \\ &\overset{(ii)}{=} \lambda_{V_0} \otimes \lambda_A \\ &= 1 \otimes \lambda_A = 1 \otimes r_A(g). \end{aligned}$$

This implies

$$\Delta \circ \lambda_V = (1 \otimes r_A(g)) \circ \Delta$$

but also

$$\Delta \circ r_V(g) = (1 \otimes r_A(g)) \circ \Delta.$$

Because of the injectivity of Δ it now follows

$$\lambda_V = r_V(g).$$

$\square$

Corollary 2. *Let $\phi : G \to H$ be any morphism of algebraic groups. Then, for all $g \in G$*

$$\begin{aligned} \phi(g)_s &= \phi(g_s) \\ \phi(g)_u &= \phi(g_u). \end{aligned}$$

Proof. Let V be any **faithful** representation of H, i.e. $r_V : H \to \mathsf{GL}(V)$ is injective, (for a finite-dim. V).

Then, $r_V \circ \phi$ is a rep. of G. To prove (i), it suffices to show

$$r_V(\phi(g)_s) = r_V(\phi(g_s))$$

since H operates faithfully on V.

We know that

$$r_V(\phi(g)_s) = r_V(\phi(g))_s$$

(characterizing property of h_s for $h \in H$). On the other hand,

$$r_V(\phi(g_s)) = (r_V \circ \phi)(g_s) = r_V(\phi(g))_s.$$

Therefore, claim (i) follows. (ii) works analogously. □

Definition 4. Let $g \in G$ where G is an algebraic group. We call g **semisimple**, if $g = g_s$.

We call g **unipotent**, if $g = g_u$.

Lemma 14. *For $g \in G$, the following are equivalent:*

(i) g is semisimple.

(ii) $r_V(g)$ is semisimple for all finite-dim. rep. V.

(iii) $r_V(g)$ is semisimple for at least one faithful f.d. rep. V of G.

We get an analogous lemma for unipotent group elements.

Proof. We have

$$\begin{aligned} (i) &\iff g = g_s \\ &\overset{\text{Def. of } g_s \text{ by goal thm.}}{\iff} r_V(g) = r_V(g)_s \forall \text{ f.d. } V \\ &\iff r_V(g) \text{ is semisimple} \\ &\iff (ii) \implies (iii). \end{aligned}$$

On the other hand,

$$(iii) \implies \exists \text{ faithful f.d. } V \text{ s.t. } r_V(g) = r_V(g)_s = r_V(g_s) \implies g = g_s.$$

□

0.2 Non-Commutative Algebra

Definition 5. A **ring** R (for now) is unital, associative but not necessarily commutative.

Example 5. The ring of matrices over some field or ring.

Definition 6. A **left ideal** $I \subset R$ is a subset that is an abelian subgroup of $(R, +)$ s.t.$ra \in I$ for all $r \in R, a \in I$.

A **right ideal** $I \subset R$ is a subset that is an abelian subgroup with

$$IR \subset I.$$

A two-sided ideal I is a subset that is a left and a right ideal of R.

It is easy to check that for any homomorphism of rings $\phi : R \to S$, $\mathsf{Kern}\phi$ is a two-sided ideal. Also, if $J \subset R$ is any two-sided ideal, then there exists a unique ring structure on R/J s.t. the projection $R \to R/J$ is a ring homomorphism.

Definition 7. A **left module** M for R is an abelian group equipped with a ring homomorphism

$$R \xrightarrow{\alpha} \mathsf{End}(M)$$

where $\mathsf{End}(M)$ acts on the left of M. We write

$$rm := \alpha(r)m.$$

We have

$$(r_1 r_2)(m) = r_1(r_2(m)).$$

If R **acts** on M by the right, we write

$$R \curvearrowright M.$$

Example 6. $M_n(k) \curvearrowright k^n$ where k^n is the space of column vectors.

If k^n denotes the space of row vectors, we have $k^n \curvearrowleft M_n(k)$.

Definition 8. A **(left) submodule** $N \subset M$ is an algebraic subgroup s.t.

$$RN \subset N.$$

It follows that N is itself is a left module.

Definition 9. A (left) module M of R is **simple** (or irreducible) if it has exactly the two submodules: $0 = \{0\}$ and M.

Definition 10. A ring R is a **division ring** if it satisfies any of the following equivalent requirements:

(i) $R^\times = R \setminus \{0\}$ where $R^\times = \{r \in R \mid \exists a, b \in R : ar = rb = 1.\}$

(ii) R has no nontrivials left or right ideals.

Definition 11. If $R \curvearrowright M$, then we can define

$$\mathsf{End}_R(M) := \{\phi \in \mathsf{End}(M) \mid \phi(rm) = r\phi(m)\ \forall r \in R, m \in M\}.$$

Note, that $\mathsf{End}_R(M)$ is a ring.

Lemma 15 (Schur's Lemma)**.** *If M is simple, then $\mathsf{End}_R(M)$ is a division ring.*

Lemma 16. *Let k be a field. Then, $M_n(k)$ has no nontrivial twosided ideals.*

Theorem 6 (Jacobson Density Theorem (Double Commutant Theorem))**.** *Suppose M is a simple left module which is finitely generated as a right D-module for $D = \mathsf{End}_R(M)$.*

Assume that R acts faithfully on M, i.e. $R \to \mathsf{End}_R(M)$ is injective.

Then, the map $R \to \mathsf{End}_D(M)$ is an isomorphism.

[0] If $ar = rb = 1$, then $a = arb = b$.