Jordan decomposition and Tannaka duality

Raymond van Bommel, rbommel@math.leidenuniv.nl

These informal talk notes are mostly due to [1] and are prone to errors. I can also recommend sections 2.4 and 2.5 of [2].

1 Jordan decomposition

1.1 Case of finite dimensional vector spaces

Let k be a perfect field, let V be a finite dimensional k-vector space and let $\alpha : V \to V$ be a k-automorphism. Then α is called *diagonalizable* if V has a basis of eigenvectors, α is called *semisimple* if $\alpha \otimes K$ is diagonalizable for some field extension K/k, α is called *nilpotent* if $\alpha^m = 0$ for some $m \in \mathbb{Z}_{\geq 0}$, and α is called *unipotent* if $\alpha - 1$ is nilpotent. Let $E = E(\alpha)$ be the set of eigenvalues of α in k and for $a \in E$ let $V^a := \{v \in V : \exists N : (\alpha - a)^N v = 0\}$ be the associated generalized eigenspace.

Proposition 1. *If all eigenvalues of α lie in k, then*

$$V = \bigoplus_{a \in E} V^a.$$

Proof. Omitted, see proposition 2.1 of [1, p. 155]. □

Theorem 2 (Jordan decomposition)**.** *There exist unique k-automorphisms $\alpha_s, \alpha_u : V \to V$ such that α_s is semisimple, α_u is unipotent, and $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$.*

Proof. First we prove the uniqueness. Suppose that $\alpha_s \circ \alpha_u$ and $\beta_s \circ \beta_u$ are two such decomposition, then $\beta_s^{-1} \circ \alpha_s = \beta_u \circ \alpha_u^{-1}$ is semisimple and nilpotent, hence it is equal to the identity map. This proves the uniqueness.

For the existence first consider the case where all eigenvalues are in k. By proposition 1 we have $V = \bigoplus_{a \in E} V^a$. Let $\alpha_s : V \to V$ be such that $\alpha|_{V^a}$ is the multiplication by a. Now, let $\alpha_u := \alpha \circ \alpha_s^{-1}$. Then α_s is semisimple by construction, α_u is unipotent because all its eigenvalues are 1 and α_s and α_u commute. This proves the existence when all eigenvalues are in k.

In the general case the eigenvalues lie in a finite field extension K/k. Because k is perfect, we may and do assume that K/k is finite Galois with Galois group G. Let $\alpha_s \circ \alpha_u$ be the Jordan decomposition of $\alpha \otimes K$. Then it is easy to check that $(\sigma\alpha_s) \circ (\sigma\alpha_u)$ is also a Jordan decomposition for all $\sigma \in G$. Hence, $\sigma\alpha_s = \alpha_s$ and $\sigma\alpha_u = \alpha_u$. Hence α_s and α_u are defined over k and the Jordan decomposition of α is $\alpha_s|_V \circ \alpha_u|_V$. □

Lemma 3. *Let α and β be k-automorphisms of finite dimensional k-vector spaces V and W. Let $\phi : V \to W$ be a k-morphism. Suppose that $\phi\circ\alpha = \beta\circ\phi$. Then we have $\phi \circ \alpha_s = \beta_s \circ \phi$ and $\phi \circ \alpha_u = \beta_u \circ \phi$.*

Proof. It suffices to prove this in the case where all eigenvalues are in k. Let $a \in E(\alpha)$. Then it is easy to check that $\phi(V^a) \subset W^a$. Hence, on V^a the maps $\phi \circ \alpha_s$ and $\beta_s \circ \phi$ agree. The same is true for $\phi \circ \alpha_s^{-1}$ and $\beta_s^{-1} \circ \phi$. Hence by proposition 1 the maps agree on V. □

Corollary 4. *Let W be a subspace of V, then $\alpha|_W = \alpha_s|_W \circ \alpha_u|_W$ is the Jordan decomposition of $\alpha|_W$.*

Lemma 5. *Let α and β be k-automorphisms of finite dimensional k-vector spaces V and W. Then $(\alpha \otimes \beta)_s = \alpha_s \otimes \beta_s$ and $(\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u$.*

Proof. Similar to the proof of lemma 3, see proposition 2.5 of [1, p. 157]. □

1.2 Case of infinite dimensional vector spaces

Let k be a perfect field and V an arbitrary k-vector space. A k-automorphism $\alpha : V \to V$ is called *locally finite* if V is a union of finite dimensional α-stable subspaces. The notions of a semisimple, nilpotent and unipotent automorphism extend.

Theorem 6 (Jordan decomposition)**.** *Theorem 2 also holds for arbitrary V and locally finite α.*

Proof. Every α-stable subspace has a unique Jordan decomposition and these coincide by corollary 4. □

1.3 Case of algebraic groups

Theorem 7 (Jordan decomposition in algebraic groups)**.** *Let G be an affine algebraic group over a perfect field k. For any $g \in G(k)$ there are unique $g_s, g_u \in G(k)$ such that for all (locally finite) representations $r : G \to \mathbf{Aut}(V)$ we have $r(g_s) = r(g)_s$ and $r(g_u) = r(g)_u$. Furthermore $g_s g_u = g_u g_s = g$.*

Proof. The theorem follows from Tannaka duality applied to the family $(r(g)_s)_r$ and $(r(g)_u)_r$ where r ranges over all finite dimensional representations. By choosing a faithful representation r we find $r(g) = r(g_s)r(g_u) = r(g_u)r(g_s)$ and hence the desired equality. □

2 Tannaka duality

Let G be an affine algebraic group over a field k (in fact we can do this over a noetherian ring k) with coordinate ring A and let R be a k-algebra.

2.1 Statement

Tannaka duality allows us to reconstruct the group G when we only have some limited knowledge about its representations.

Theorem 8 (Tannaka duality)**.** *Suppose that for every representation $r_V : G \to \mathbf{Aut}(V)$ which is finitely generated as k-module we have an $\alpha_V : V_R \to V_R$ such that*

(a) if V and W are representations, then $\alpha_{V \otimes W} = \alpha_V \otimes \alpha_W$;

(b) if $\phi : V \to W$ is a homomorphism of G-modules then $\phi_R \circ \alpha_V = \alpha_W \circ \phi_R$;

(c) $\alpha_k = 1$.

Then there exists a unique $g \in G(R)$ such that $\alpha_V = r_V(g)$ for every V.

Proof of theorem 7. The conditions (a), (b) and (c) are satisfied because of lemmas 5 and 3. □

2.2 Some lemmas

Let $\Delta : A \to A \otimes A$ be the comultiplication. Furthermore let $r_A : G \to \mathbf{End}_A$ be the regular representation, i.e. for every k-algebra R we let $g \in G(R)$ act on $f \in A$ by

$$\forall x \in G(R) : (gf)_R(x) = f_R(x \cdot g),$$

where we consider $f \in A$ as regular function $G \to k$. To prove theorem 8 we need the following lemmas.

Lemma 9. *Let $u : A \to A$ be a k-algebra endomorphism such that $\Delta \circ u = (1 \otimes u) \circ \Delta$. Then there exists a $g \in G(k)$ such that $u = r_A(g)$.*

Proof. Let $\phi : G \to G$ be the morphism corresponding to u. Let $m : G \times G \to G$ be the multiplication (corresponding to Δ). Then we have

$$\phi_R(x \cdot y) = \phi_R(m_R(x, y)) = m_R(x, \phi_R(y)) = x \cdot \phi_R(y). \tag{1}$$

By choosing $y = e$ in (1) we find $\phi_R(x) = x \cdot g$ where $g = \phi_R(e)$. Then the correspondence yields us that $u = r_A(g)$. □

Lemma 10. *Every representation V of G is a union of its finitely generated subrepresentations, or otherwise stated representations of G are locally finite.*

Proof. Already given on 19 February, see proposition 6.6 in [1, p. 121]. □

Lemma 11. *Let $r_V : G \to \mathbf{Aut}(V)$ be a representation of G finitely generated as k-module. Let V_0 be the underlying k-module. Then there is an injective G-morphism $\rho : V \to V_0 \otimes A$.*

Proof. It is easy to check that the coaction $V_0 \otimes \Delta$ of $V_0 \otimes A$ commutes with the comultiplication Δ, hence ρ is a homomorphism. The injectivity follows from the fact that $(\mathrm{id}_V \otimes \epsilon) \circ \rho$ is injective. □

2.3 Proof

Proof of theorem 8. By combining (b) and lemma 10 we can extend our family (α_V) to range over all representations V instead of only the finitely generated.

Let $A' = A \otimes R$, and let $\alpha' = \alpha_{A'}$ be the R-linear map belong the the regular representation r of G on A'. The multiplication $m : A' \otimes A' \to A'$ is a G-morphism for the representations $r \otimes r$ and r, because for all $x \in G(R)$ and $f \otimes f' \in A' \otimes A'$ we have

$$(r(g) \circ m)(f \otimes f')(x) = (r(g)(f \cdot f'))(x) = (ff')(xg)$$
$$(m \circ (r(g) \otimes r(g)))(f \otimes f')(x) = ((r(g)f) \cdot (r(g)f'))(x) = f(xg) \cdot f'(xg).$$

By (a) and (b) we then get that $m \circ \alpha' = (\alpha' \otimes \alpha') \circ m$, i.e. that α' is a k-algebra morphism. Similarly $\Delta : A' \to A' \times A'$ is a G-morphism for the representation r and $1 \otimes r$. Hence, by (a) and (b) we get $\Delta \circ \alpha' = (1 \otimes \alpha') \circ \Delta$. Now we may apply lemma 9 to G_R to conclude that $\alpha' = r_A(g)$ for some $g \in G(R)$.

Now, we will proof that this g is indeed the G we are looking for. Let $r_V : G \to \mathbf{Aut}(V)$ be a representation of G that is finitely generated as k-module. Let V_0 be the underlying k-module. Then by lemma 11 we have an injective map $\rho : V \to V_0 \otimes A$. By definition of g we know that α and $r(g)$ agree on A and they agree on V_0 by (c). By (a) they then agree on $V_0 \otimes A$ and by (b) they agree on V, which is what we wanted to proof.

The existence of g is proven. The uniqueness can be deduced by noticing that the regular representation is faithful. □

References

[1] J.S. Milne. *Basic Theory of Affine Group Schemes.* `http://www.jmilne.org/math/CourseNotes/`, 2013.

[2] T.A. Springer. *Linear Algebraic Groups.* Modern Birkhäuser Classics, 2nd edition, 1998.