CONJUGACY CLASSES OF SEMISIMPLE ELEMENTS IN AN ALGEBRAIC GROUP AND ITS ASSOCIATED FINITE GROUPS

JAY TAYLOR

Let $k = \overline{\mathbb{F}_p}$ for some prime $p > 0$ and let G be a connected reductive algebraic group.

1. Er ... Algebraic Group?

A **linear algebraic group** G is a group with an added topological structure, known as the Zariski topology. In essence it is a group which can be defined as the vanishing points, in k^n, of some polynomials in $k[X_1, \dots, X_n]$ and whose multiplication and inversion maps are continuous with respect to the topology. We define the Zariski topology on G by defining closed sets to be precisely those which can be defined as the vanishing points of a set of polynomials.

For example all our favourite matrix groups are linear algebraic groups. We naturally associate $\mathrm{M}_n(k)$ with the space $k^n \times k^n \cong k^{n^2}$ and then consider polynomials in $k^{n^2}[X_{ij} \mid 1 \leqslant i, j \leqslant n]$. A good example is the special linear group. We know that we can describe, for $X \in \mathrm{M}_n(k)$, the determinant of X as a polynomial in the following way

$$\det(X) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{n\sigma(n)} \in k^{n^2}[X_{ij} \mid 1 \leqslant i, j \leqslant n].$$

Then we define the special linear group over k as

$$\mathrm{SL}_n(k) = \{(x_{ij}) \in k^{n^2} \mid \det(x_{ij}) - 1 = 0\}.$$

For most purposes in algebraic groups we deal with special kinds of algebraic groups known as **connected reductive** algebraic groups.

Definition. The **radical** of G, denoted $R(G)$ is the maximal closed connected solvable normal subgroup of G. The **unipotent radical** of G, denoted $R_U(G)$, is the maximal closed connected unipotent normal subgroup of G.

Now, we say G is **reductive** if $R_U(G) = \{1\}$ and G is **semisimple** if $R(G) = \{1\}$. We note that as $R_U(G) \subseteq R(G)$ we have G semisimple $\Rightarrow$ G reductive. In general it is more than sufficient to think of $\mathrm{GL}_n(k)$ when hearing the words connected reductive algebraic group. You may be slightly concerned that $\mathrm{GL}_n(k)$ is in fact not defined as the vanishing of some polynomial equations. However we fix this in the following way

$$\mathrm{GL}_n(k) = \{(x_{ij}, y) \in k^{n^2} \times k \mid \det(x_{ij})y - 1 = 0\}.$$

A connected reductive algebraic group comes with a very important structure known as a BN-pair or Tits system. In the following we will define the elements of this that we will need to continue with this talk and in parallel describe what these things look like in $\mathrm{GL}_n(k)$. If at all lost just think of what the matrices look like in $\mathrm{GL}_n(k)$.

Terminology	$\mathrm{GL}_n(k)$
Let B be a **Borel subgroup** of G. This is a maximal closed connected solvable subgroup of G.	$\begin{pmatrix} \star & \cdots & \star \\ & \ddots & \vdots \\ & & \star \end{pmatrix}$
Let U be the **unipotent radical** of B.	$\begin{pmatrix} 1 & \cdots & \star \\ & \ddots & \vdots \\ & & 1 \end{pmatrix}$
Let T be a **maximal torus** of G. This is a maximal subgroup of G, which is isomorphic to $k^\times \times \cdots \times k^\times$.	$\begin{pmatrix} \star & & \\ & \ddots & \\ & & \star \end{pmatrix}$

Fact. *Every maximal torus of G lies in a Borel subgroup of G but this is not necessarily unique. See Corollary A, Section 21.3 of* [Hum75]. *For example the maximal torus of diagonal matrices in* $\mathrm{GL}_n(k)$ *lies in the subgroup of upper triangular matrices and the subgroup of lower triangular matrices.*

Now as a part of the definition of a BN-pair we have that, for a connected reductive algebraic group, $W := N_G(T)/T$ will always be a Weyl group, where $N_G(T)$ is the normaliser of the torus in G. In fact for a connected reductive algebraic group this is always finite. The associated Weyl group of G is very important and really controls most of the defining features of the algebraic group.

Example. Let $G = \mathrm{GL}_n(k)$ and T be the maximal torus of diagonal matrices. Then $N_G(T)$ is the group of all monomial matrices in $\mathrm{GL}_n(k)$. Therefore we can see that $N_G(T)/T \cong \mathfrak{S}_n$.

We now need a very important fact in the theory of algebraic groups.

Fact. *Any algebraic group G can be embedded into* $\mathrm{GL}_n(k)$ *for some n. See Corollary 2.4.4 of* [Gec03].

So, just like any group can be embedded into the symmetric group we have any algebraic group can be embedded into $\mathrm{GL}_n(k)$. This fact allows us the following definition

Definition. We define a morphism of $\mathrm{GL}_n(k)$ by

$$\begin{aligned} F_q : \mathrm{GL}_n(k) &\to \mathrm{GL}_n(k) \\ (a_{ij}) &\mapsto (a_{ij}^q), \end{aligned}$$

where $q = p^e$ for some $0 < e \in \mathbb{N}$. A **standard Frobenius** map of an algebraic group G is any map $F : G \to G$ such that there exists an embedding $\iota : G \to GL_n(k)$ which satisfies

$\iota \circ F = F_q \circ \iota$ for some q. A morphism $F : G \to G$ is called a **Frobenius** map if for some $m \in \mathbb{N}$ we have F^m is a standard Frobenius map.

If $F : G \to G$ is a Frobenius map then we can consider the fixed point group of F which we denote

$$G^F := \{g \in G \mid F(g) = g\}.$$

Fact. *G^F is always a finite subgroup of G. See Proposition 4.1.4 of* [Gec03].

Example. We think of $\mathrm{GL}_n(k)$, where $k = \overline{\mathbb{F}_p}$, and the standard Frobenius map F_q where $q = p^e$. Then we have $G^{F_q} = \mathrm{GL}_n(q)$, i.e. the finite general linear group defined over the field $\mathbb{F}_q$.

2. So, semisimple you say?

We have two ways to define semisimple elements in an algebraic group when our field is of positive characteristic these are equivalent.

Definition. Let $\iota : G \to \mathrm{GL}_n(k)$ be an embedding of G into $\mathrm{GL}_n(k)$ for some appropriate n. Then an element $s \in G$ is **semisimple** if $\iota(s)$ is a semisimple, (i.e. diagonalisable because our field is algebraically closed), matrix.

Definition. An element $s \in G$ is called **semisimple** if its order is prime to p.

For our example of $\mathrm{GL}_n(k)$ it will be more constructive to consider the first definition as it will make the following facts slightly more believable.

Fact. *All maximal tori of G are conjugate in G. See Corollary A, section 21.3 of* [Hum75].

Fact. *Every semisimple element of G lies in a maximal torus of G. See Corollary, section 19.3 of* [Hum75].

If we think about this in $\mathrm{GL}_n(k)$ then this may make some sense. Consider the maximal torus of diagonal matrices in $\mathrm{GL}_n(k)$. Then a semisimple matrix, over an algebraically closed field, is one which is conjugate to a diagonal matrix. Hence every semisimple element in $\mathrm{GL}_n(k)$ has a conjugate which lies in the maximal torus of diagonal matrices. In fact a maximal torus is made up entirely of semisimple elements.

Now we recall the Weyl group $W = N_G(T)/T$. We have a natural action of the Weyl group on the maximal torus by conjugation. Then with this action we can state the following theorem.

Theorem. *We have that for two elements $t_1, t_2 \in T$ that t_1, t_2 are conjugate in G if and only if they lie in the same W orbit. Hence there is a bijection between semisimple conjugacy classes in G and orbits T/W of the Weyl group acting on T.*

Proof. This result uses the fact that in a group with a split BN-pair we have a unique way of writing an element as a product of things coming from $R_U(B)$, T and W. See section 2.5 of [Car85] for more details on the unique expression and section 3.7 of [Car85] for the proof of the theorem. □

Example. Consider the group $\mathrm{GL}_3(k)$. We have the standard maximal torus T of diagonal matrices in $\mathrm{GL}_3(k)$, so we can denote a typical semisimple element in T by a triple (α, β, γ) for $\alpha, \beta, \gamma \in k$. If we assume that all these elements are distinct, then the orbits of $W \cong \mathfrak{S}_3$ acting on T look like

$$\{(\alpha,\beta,\gamma),(\alpha,\gamma,\beta),(\beta,\alpha,\gamma),(\beta,\gamma,\alpha),(\gamma,\beta,\alpha),(\gamma,\alpha,\beta)\},$$
$$\{(\alpha,\alpha,\beta),(\alpha,\beta,\alpha),(\beta,\alpha,\alpha)\},$$
$$\{(\alpha,\alpha,\alpha)\}.$$

Therefore we have seemingly taken a very infinite problem and reduced it to something that is finite. For example in $\mathrm{GL}_n(k)$ we can take a general diagonal matrix and conjugate this with the permutation matrices of the Weyl group. This will give us the conjugacy class of this semisimple element in $\mathrm{GL}_n(k)$.

So in a connected reductive algebraic group G we have a nice solution to this problem. All we have to do is examine the orbits of the action of the Weyl group on a maximal torus and we're done. However, when we pass to the finite group this situation becomes slightly more complicated.

3. Finite, schminite.

We now want to take our very nice solution in G and pass this to G^F. However what we're essentially doing is taking a conjugacy class in a group and trying to see what happens to it when we intersect it with a subgroup. For example in the symmetric group we know that conjugacy classes are represented by cycle type but in the alternating group it can happen that these conjugacy classes split. The same thing will happen in our finite subgroup G^F and ideally we would like to know how, why and when they will split.

Definition. We say $x \in G$ is F-stable if $F(x) = x$. We say a subset $H \subseteq G$ is **F-stable** if $F(H) = H$, note that this does not mean every element of H is F-stable.

Fact. *There exists F-stable Borel subgroups and maximal tori of G. See section 1.17 of* [Car85].

Definition. Let T be an F-stable maximal torus of G. Then we say the subgroup $T^F = \{t \in T \mid F(t) = t\} \leqslant G^F$ is a **maximal torus** of G^F.

Note that T^F is just an abelian subgroup of G^F, it is not necessarily maximal in G^F. Now we know that in G all maximal tori are conjugate. However if T_1 and T_2 are two F-stable maximal tori of G it is not true that we can find an element $g \in G^F$ such that T_1 and T_2 are conjugate by g. This causes us our first problem In fact not every F-stable maximal torus of G lies in an F-stable Borel subgroup but every F-stable Borel subgroup does contain an F-stable maximal torus.

We need the important idea of F-conjugacy. Consider the Weyl group W. We say that $w, w' \in W$ are **F-conjugate** if there exists $x \in W$ such that $w' = x^{-1}wF(x)$. We have

F-conjugacy is an equivalence relation on W. We call the equivalence classes under this relation F-conjugacy classes.

The first step on the road to solving our problem is the following theorem.

Theorem. *There is a bijection between the G^F conjugacy classes of F-stable maximal tori of G and the F-conjugacy classes of W.*

Proof. See Proposition 3.3.3 in [Car85] □

Now we note that if F acts trivially on the Weyl group then the F-conjugacy classes of W are in fact just the regular conjugacy classes of W. This happens in $\mathrm{GL}_n(k)$. Consider F_q the standard Frobenius map then we have an element of W is just a permutation matrix but applying F_q to this will leave it unchanged.

We briefly wish to talk about centralisers of semisimple elements because of the following. Let $s \in G^F$ be semisimple and $g \in G$ such that ${}^g s := gsg^{-1} \in G^F$ then $g^{-1}F(g) \in C_G(s)$. This is clear because

$$gsg^{-1} = F(gsg^{-1}) = F(g)sF(g^{-1}) \Rightarrow g^{-1}F(g)s = sg^{-1}F(g).$$

Now if ${}^g s = {}^h s$ for some $h \in G$ we have $g^{-1}F(g)$ and $h^{-1}F(h)$ are F-conjugate in $C_G(s)$. This is because ${}^g s = {}^h s \Rightarrow {}^{h^{-1}g} s = s \Rightarrow h^{-1}g \in C_G(s)$ and clearly

$$g^{-1}F(g) = g^{-1}h(h^{-1}F(h))F(h^{-1}g).$$

In fact we obtain the following result

Theorem. *The map taking $g \mapsto {}^g s$ for $g^{-1}F(g) \in C_G(s)$ induces a bijection between F-conjugacy classes of $C_G(s)/C_G(s)^\circ$ and G^F orbits of F-stable conjugates of s in G.*

Proof. This is proved in a more general statement in Theorem 4.3.5 of [Gec03]. □

This result suggests that knowledge about the centralisers of a semisimple element and whether it is connected or not will prove most useful to us. In fact this result says that if $C_G(s)$ is connected then the F-stable conjugates of s will form a single G^F conjugacy class of semisimple elements.

Theorem. *Let s be a semisimple element of G and T a maximal torus of G containing s. Then*

(a) $C_G(s)^\circ = \langle T, X_\alpha \mid \alpha(s) = 1\rangle$,
(b) $C_G(s) = \langle T, X_\alpha, \dot{w} \mid \alpha(s) = 1, {}^{\dot{w}} s = s\rangle$.

where X_α are the root subgroups with respect to the torus T and $\dot{w}$ is a representative of the Weyl group element w in $N_G(T)$.

Proof. See Theorem 3.5.3 of [Car85]. □

Now in the above theorem we said that X_α are the root subgroups. It is not really important to know what the root subgroups are, just know that they are 1-dim subgroups isomorphic to k^+ associated to each root in the root system. They have the property that G is generated by a maximal torus and the root subgroups. The important thing to notice about the above result is that $C_G(s)/C_G(s)^\circ$ will be isomorphic to a group generated by representatives of the Weyl group. So F-conjugacy classes of $C_G(s)/C_G(s)^\circ$ will in fact just be related to F-conjugacy classes of the Weyl group.

With this in mind we now state a very important result due to Steinberg.

Theorem (Steinberg)**.** *Let G be a connected reductive group whose derived subgroup G' is simply-connected. Let s be a semisimple element of G. Then $C_G(s)$ is connected.*

Proof. See Theorem 3.5.6 of [Car85]. □

So in a simply connected algebraic group we will have that given an F-stable conjugacy class of semisimple elements, say C, in G that C^F will form precisely one conjugacy class of semisimple elements in G^F. Finally with this in place we can state the main result regarding semisimple conjugacy classes in G^F.

Theorem. *Suppose G is a connected reductive group whose derived group G' is simply connected. Then there is a bijection between semisimple conjugacy classes of G^F and F-stable orbits in T/W. Furthermore the number of semisimple conjugacy classes in G^F is $|(Z(G)^\circ)^F|q^\ell$, where ℓ is the semisimple rank of G.*

Proof. See Proposition 3.7.3 and Theorem 3.7.6 of [Car85]. □

We note that simply connected refers to the classification of simple algebraic groups. An example of the above is $\mathrm{GL}_n(k)$. We have $\mathrm{GL}_n(k)$ is a connected reductive algebraic group whose derived subgroup is $\mathrm{SL}_n(k)$ which is a semisimple simply connected algebraic group of type A_{n-1}.

Example. We consider $G = \mathrm{GL}_2(k)$ together with $F = F_q$ the standard Frobenius map and hence $G^F = \mathrm{GL}_2(q)$. Let λ be a primitive (q^2-1)th root of unity in k then $\eta = \lambda^{q+1}$ is a primitive $(q-1)$th root of unity in k. We have $\mathrm{GL}_2(k)$ is an algebraic group of type A_1 and hence there are only two roots. With respect to the standard maximal torus T these are

$$\alpha \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} = xy^{-1} \qquad\qquad -\alpha \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} = x^{-1}y.$$

The Weyl group W is isomorphic to $\mathfrak{S}_2$. We can see this as we have $N_G(T)/T$ is given by the coset representatives

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} T \qquad\qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} T$$

We have the orbits of the Weyl group acting on the standard maximal torus are

$$\{(x,y),(y,x)\} \qquad\qquad \{(x,x)\},$$

where $x \neq y \in k$ and (x,y) represents a diagonal matrix in T.

We now consider when these orbits are F-stable. The latter orbit is F-stable if and only if $x^q = x \Rightarrow x^{q-1} = 1$ and hence $x = \eta^i$ for some $0 \leqslant i \leqslant q-2$. There are $q-1$ choices for i and so we get $q-1$ different conjugacy classes in $\mathrm{GL}_2(q)$. Now this element is in the centre of $\mathrm{GL}_2(q)$ and so clearly $C_G(s) = \mathrm{GL}_2(q)$. Now also we see that $\pm\alpha(\eta^i, \eta^i) = 1$ and so $C_G(s) = \langle T, X_\alpha, X_{-\alpha}\rangle = \mathrm{GL}_2(k) \Rightarrow C_G(s)^F = C_{G^F}(s) = \mathrm{GL}_2(q)$.

There are two possibilities for the first orbit to be F-stable. The first possibility is that $x^q = x$ and $y^q = y$, which means $x = \eta^i$ and $y = \eta^j$ for some $0 \leqslant i, j \leqslant q-2$ with $i \neq j$. We have $q-1$ choices for i and $q-2$ choices for j, dividing through by the size of the orbit we have $\frac{(q-1)(q-2)}{2}$ different conjugacy classes in $\mathrm{GL}_2(q)$. We have $\pm\alpha(\eta^i, \eta^j) \neq 1$ when $i \neq j$ and so $C_G(s) = \langle T\rangle = T$. Therefore $C_{G^F}(s) = T^F \cong \mathbb{Z}_{q-1} \oplus \mathbb{Z}_{q-1}$, which means $|C_{G^F}(s)| = (q-1)^2$.

The second possibility is that we could have $x^q = y$ and $y^q = x \Rightarrow x^{q^2} = x \Rightarrow x^{q^2-1} = 1$ and so $x = \lambda^i$, $y = \lambda^{iq}$ for some $0 \leqslant i \leqslant q^2-2$. Recall that $\lambda^{q+1} = \eta$ and so if $q+1 \mid i$ we will have that $(\lambda^i, \lambda^{iq})$ is one of the cases we have already considered. We have q^2-1 choices for i but we also have $q-1$ choices for j such that $i = (q+1)j$, (we really have q choices for j but we don't want to throw away $j = 0$), so we have $q^2-1-(q-1) = q^2-q = q(q-1)$ choices for i. Dividing through by the order of the orbit this gives us $\frac{q(q-1)}{2}$ different conjugacy classes in $\mathrm{GL}_2(q)$. We have $\pm\alpha(\lambda^i, \lambda^{iq}) \neq 1$ and so $C_G(s) = T$.

Now the element $(\lambda^i, \lambda^{iq})$ is not F-stable. However recall that we have a conjugacy class of maximal tori in $\mathrm{GL}_2(q)$ corresponding to the non-identity element in W. Therefore we have a conjugate maximal torus ${}^gT$, such that $g^{-1}F(g)$ is the non-identity element in W, which is not conjugate in G^F to T^F. This semisimple element lies in the non-split maximal torus and so ${}^g(\lambda^i, \lambda^{iq})$ is F-stable for some $g \in G$. Therefore the centraliser of this element in $\mathrm{GL}_2(q)$ will be the other maximal torus which we denote $T^{Fw^{-1}}$ which has order $(q-1)(q+1) = q^2-1$.

Therefore the following table gives the information regarding the semisimple classes in $\mathrm{GL}_2(q)$.

s	No. Classes	No. Elements	$C_{G^F}(s)$	$\lvert C_{G^F}(s)\rvert$
(η^i, η^i)	$q-1$	1	$\mathrm{GL}_2(q)$	$q(q^2-1)(q-1)$
(η^i, η^j)	$\frac{(q-1)(q-2)}{2}$	$q(q+1)$	T^F	$(q-1)^2$
$(\lambda^i, \lambda^{iq})$	$\frac{q(q-1)}{2}$	$q(q-1)$	$T^{Fw^{-1}}$	q^2-1

Note that $Z(G)^\circ = \{\lambda I_2 \mid \lambda \in k\}$ and so $(Z(G)^\circ)^F = \{\eta^i I_2 \mid 0 \leqslant i \leqslant q-2\}$. Therefore we should have $(q-1)q$ conjugacy classes of semisimple elements in $\mathrm{GL}_2(q)$. Indeed we have

$$q-1+\frac{(q-1)(q-2)}{2}+\frac{q(q-1)}{2} = \frac{2q-2+q^2-3q+2+q^2-q}{2}, \\ = (q-1)q,$$

semisimple classes in $\mathrm{GL}_2(q)$.

References

[Car85] Roger W. Carter. *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*. John Wiley & Sons Ltd., 1985.

[Gec03] Meinolf Geck. *An Introduction to Algebraic Geometry and Algebraic Groups*. Oxford University Press, 2003.

[Hum75] James E. Humphreys. *Linear Algebraic Groups*. Springer-Verlag, 1975.