Finite groups of Lie type

Steinberg [*Endomorphisms of linear algebraic groups,* **1968**] has studied the situation where G is a reductive algebraic group over an algebraically closed field and F is an algebraic endomorphism such that G^F (the fixed points) is finite. Then G^F is called a *finite group of Lie type*.

He has classified the possibilities. If G is simple then it is an algebraic group over the algebraic closure $\overline{\mathbb{F}}_q$ of a finite field $\mathbb{F}_q$, and

- either F is the Frobenius attached to an $\mathbb{F}_q$-structure,
- or G is of type B_2, F_4 or G_2 and F^2 is a Frobenius attached to an $\mathbb{F}_q$-structure.

In the first two of the last cases q is a power of 2 and in the third case a power of 3; the groups G^F in these cases where discovered by Suzuki and Ree.

What is a Frobenius?

Let q be a power of the prime p.
On the affine line $\mathbb{A}_1 = \operatorname{Spec}(\overline{\mathbb{F}}_q(T))$ we have the Galois action $\sum a_i T^i \mapsto \sum a_i^q T^i$. Since in characteristic p we have $(a+b)^q = a^q + b^q$ the algebraic morphism given by $T \mapsto T^q$, *i.e.* $\sum a_i T^i \mapsto \sum a_i T^{qi}$ has the same fixed points as the Galois action, since the composed is just $\sum a_i T^i \mapsto (\sum a_i T^i)^q$.
It is called the *Frobenius* morphism.

In general an affine variety Spec A where A is an $\overline{\mathbb{F}}_q$-algebra has an $\mathbb{F}_q$-structure if $A = A_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ where A_0 is an $\mathbb{F}_q$-algebra. This structure is equivalently given by the Frobenius $a \otimes \lambda \mapsto a^q \otimes \lambda$; we recover A_0 as $\{x \mid F(x) = x^q\}$.
Another morphism F' is the Frobenius associated to another $\mathbb{F}_q$-structure iff there exists n such that $F^n = F'^n$.
Example: On $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ the standard Frobenius sends a matrix $\{a_{ij}\}$ to $\{a_{ij}^q\}$, and the fixed points are $\mathrm{GL}_n(\mathbb{F}_q)$.

Lang-Steinberg theorem

Theorem (Lang-Steinberg)

If F is an algebraic endomorphism of the affine connected algebraic group G such that G^F is finite, then the map $x \mapsto xF(x^{-1})$ is surjective.

Equivalently $H^1(F, G) = 1$. Indeed $H^1(F, G)$ is the set of F-conjugacy classes of G, where F-conjugacy of x by y sends x to $yxF(y^{-1})$.

Note that it results form Steinberg's classification that any $g \in G$ is stable by F^m for m large enough (since it is defined over some finite field, and a power of F is a Frobenius); it also follows that gF still has finitely many fixed points (since a power is a Frobenius).

Corollary

Corollary (of Lang-Steinberg)

If G is not connected we have $H^1(F, G) = H^1(F, G/G^0)$.

Proof:

- It is clear that two F-conjugate elements of G have F-conjugate images in G/G^0, thus we have natural surjective map $H^1(F, G) \to H^1(F, G/G^0)$.
- Conversely, if g and g' are F-conjugate modulo G^0, we have $hg = xg'F(x^{-1})$ for some $h \in G^0$ and $x \in G$.
  Now we may apply the Lang-Steinberg theorem in G^0 with the morphism gF to write $h = y^{-1}gF(y)g^{-1}$, whence $g = yxg'F(x^{-1}y^{-1})$ so g and g' are F-conjugate.

Actually, if H is a normal subgroup of G, we have an exact sequence

$$1 \to H^F \to G^F \to (G/H)^F \to H^1(F, H) \to H^1(F, G) \to H^1(F, G/H)$$

so if H is connected we have $(G/H)^F = G^F/H^F$.

Another corollary

Corollary

Suppose the connected algebraic group G acts on the algebraic variety X in an F-equivariant way, i.e. F acts on X and $F(g(x)) = F(g)(F(x))$, and transitively. Then

- $X^F \neq \emptyset$
- *and the G^F-orbits of G on X^F are in bijection with $H^1(F, C_G(x))$ where $C_G(x)$ is the stabilizer of some point $x \in X^F$.*

Proof:

- Given $x \in X$ we have $F(x) = h(x)$ for some $h \in G$. If $gF(g^{-1}) = h^{-1}$ then $F(g^{-1}(x)) = F(g^{-1})F(x) = F(g^{-1})h(x) = g^{-1}(x)$.
- We have a map from X^F to $H^1(F, C_G(x))$ as follows: given $y \in X^F$ there exists $g \in G$ such that $y = g(x)$. From $F(y) = y$ we get $g^{-1}F(g) \in C_G(x)$. We map the G^F-orbit of y to the image of $g^{-1}F(g)$ in $H^1(F, C_G(x))$. It is easy to check it is a well-defined bijective map.

Tori and Borel subgroups

A *maximal torus* is a maximal connected abelian subgroup.
Example: In GL_n, the diagonal matrices.
A maximal torus is isomorphic to $\mathbb{G}_m^n$ where n is the *rank* of G.

A *Borel subgroup* B is a maximal connected solvable subgroup. We have $B = U \rtimes T$ where U is the unipotent radical of B and T is a maximal torus.
Example: In GL_n, we may take for B the upper triangular matrices; then U =upper triangular matrices with 1's on the diagonal.

All pairs $T \subset B$ where T is a maximal torus and B a Borel subgroup are conjugate, thus there exists such an F-stable pair.
We have $N_G(B) = B$ and $N_G(T) \cap B = C_G(T) = T$, thus $N_G(T \subset B) = T$ and since T is connected $H^1(F, T) = 1$ and thus the F-stable pairs are G^F-conjugate.

The Weyl group and a reflection coset

The G^F-orbits of F-stable T correspond to
$H^1(F, N_G(T)) = H^1(F, N_G(T)/T) = H^1(F, W)$.
Example: In GL_n, we have $N_G(\text{diagonal matrices}) = \text{monomial matrices}$ and the quotient is the symmetric group $\mathfrak{S}_n$.

Let $X(T) := \mathrm{Hom}(T, \mathbb{G}_m) = \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)^n \simeq \mathbb{Z}^n$ since
$\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \{x \mapsto x^a\}_{a\in\mathbb{Z}}$.
Then $N_G(T)$ acts on $X(T)$ and T acts trivially so W acts.
W is a reflection group on $\mathbb{Q} \otimes X(T)$ and so also on $\mathbb{C} \otimes X(T) = \mathbb{C}^n$.

F acts on $X(T)$ and normalizes W. We thus have a reflection coset WF.
We assume now (automatic if G simple or equivalently W irreducible) that either F is the Frobenius attached to an $\mathbb{F}_{p^a}$-structure or F^2 is.
In the first case we set $q = p^a$ and in the second case $q = p^{a/2}$. Then $F = q\phi$ on $X(T)$ where ϕ is of finite order (2 or 3 if W is irreducible) and the reflection coset $W\phi$ is "independent of q".

Order formula

Theorem (Steinberg)

$$|G^F| = q^{\sum_{i=1}^n (d_i - 1)} \prod_{i=1}^n (q^{d_i} - \varepsilon_i)$$

where d_i is the degree of the fundamental invariants f_i of W and ε_i the eigenvalue of ϕ on f_i.

The proof of Steinberg uses the *Bruhat decomposition* $G = \coprod_{w\in W} BwB$.
Here we can write w instead of a representative in $N_G(T)$ since $B \supset T$. If $w \in W^F$ since T is connected we can choose an F-stable representative in $N_G(T)$ and we have $G^F = \coprod_{w\in W^F} B^F w B^F$.
If $B = U \rtimes T$ then $B^F w B^F = T^F U^F w U_w$ is a unique decomposition where $U_w \simeq U^F/(wU^F w^{-1})$.

- We have $|T^F| = \det(q - \phi)$,
- we have $|U^F| = q^{\sum_{i=1}^n (d_i - 1)}$,
- and there is a length $w \mapsto N(w)$ on W^F such that $|U_w| = q^{N(w)}$.

Steinberg concludes by some combinatorics on $W\phi$.

ℓ-adic cohomology

There is a nicer proof when F is a Frobenius using ℓ-adic cohomology. Choosing $\ell \not| q$, for a variety X over $\overline{\mathbb{F}}_q$ there are cohomology groups $H^i_c(X, \mathbb{Z}_\ell)$ which are finite dimensional $\mathbb{Z}_\ell$-modules, are 0 unless $0 \leq i \leq 2 \dim X$, and such that:

- If X comes from a variety X_0 over a number field then $\dim H^i_c(X, \mathbb{Z}_\ell) = \dim H^i_c(X_0, \mathbb{C})$.
- If $X = \mathbb{A}^r$ is an affine space, then $H^i_c(X, \mathbb{Z}_\ell) = 0$ unless $i = 2r$, and $H^{2r}_c(X, \mathbb{Z}_\ell) = \mathbb{Z}_\ell$.
- We have the Lefschetz formula $|X^F| = \sum_i (-1)^i \operatorname{Trace}(F \mid H^i_c(X, \mathbb{Z}_\ell))$.

Application: for any $\mathbb{F}_q$-structure on the affine space $X = \mathbb{A}^r$ we have $|X^F| = q^r$; indeed F acts on $H^{2r}_c(X, \mathbb{Z}_\ell)$ by a scalar λ. For n large enough the action of F^n is the standard action $x \mapsto x^{q^n}$ so $\lambda^n = q^{nr}$.
Thus for any unipotent group $|U(\mathbb{F}_q)| = q^{\dim U}$.

Cohomology of G/B

To compute $|G^F|$ write $G^F = B^F(G/B)^F$ and use that

The cohomology of G/B is isomorphic to the coinvariant algebra S_W.

The isomorphism multiplies the grading by 2; we have $H^i_c(G/B, \mathbb{Z}_\ell) = 0$ for i odd. It follows that $|(G/B)^F| = \operatorname{GradedTrace}(F \mid S_W)$.
Since $S \simeq S^W \otimes S_W$, we have

$$\operatorname{GradedTrace}(F \mid S_W) = \frac{\operatorname{GradedTrace}(F \mid S)}{\operatorname{GradedTrace}(F \mid S^W)} = \frac{\prod (q^{d_i}\varepsilon_i - 1)}{\det(q\phi - 1)}.$$

Since $S \simeq S^W \otimes S_W$, we have This works out to be the same as the formula above once multiplied by $|B^F|$.

Prime factors

The decomposition in prime polynomial factors of $|G^F|$ is

$$|G^F| = q^{\sum_{i=1}^{n}(d_i-1)} \prod_d \Phi_d(q)^{|a(d)|}$$

where Φ_d is the d-th cyclotomic polynomial, and $a(d) = \{i \mid \zeta_d^{d_i} = \varepsilon_i\}$, where $\zeta_d = e^{2i\pi/d}$.

Here $a(d)$ is the same set we called $a(\zeta_d)$; it does not depend on the primitive d-th root chosen since $W\phi$ is rational. There is a connection with maximal ζ_d-eigenspaces of elements of $W\phi$.

The above gives the decomposition in primes for large enough primes $\ell \neq p$, since $\gcd(\Phi_d(q), \Phi_{d'}(q))$ divides $\mathrm{lcm}(d, d')$; thus if ℓ does not divide $|W|$, it divides only one of the factors.

Φ_d-Sylows

There is a subgroup of G^F of cardinality $\Phi_d(q)^{|a(d)|}$.

Assume wF has a ζ_d-eigenspace of dimension $|a(d)|$.
Consider an F-stable torus T_w corresponding to the F-class of w.
If $T \subset B$ is F-stable this is obtained as gTg^{-1} where $g^{-1}F(g) \in N_G(T)$ has image w in W. Then g^{-1} transports (T_w, F) to (T, wF), so

- an F-stable subtorus of T_w corresponds to a wF-stable subtorus of T,
- or equivalently a wF-stable sublattice of $X(T)$.

Since wF stabilizes the lattice $X(T)$ it has a factor $\Phi_d(q)^{|a(d)|}$ in its characteristic polynomial. This corresponds to a subtorus S of T_w such that $|S^F| = \Phi_d(q)^{|a(d)|}$.

Such a subtorus S is called a Φ_d-Sylow.

Corollary of Springer-Lehrer

Theorem

- *The Φ_d-Sylows are G^F-conjugate.*
- *If S is a Φ_d-Sylow, then $N_{G^F}(S)/C_{G^F}(S)$ is a complex reflection group, with degrees $\{d_i \mid i \in a(d)\}$.*
- *The number of Φ_d-Sylows is $\equiv 1 \pmod{\Phi_d(q)}$.*
- *A Φ_d-Sylow is the product of $|a(d)|$ F-stable tori S_i such that S_i^F is a cyclic group of order $\Phi_d(q)$.*

The third item above says that $|G^F|/|C_{G^F}(S)|$, when specializing q to ζ_d, gives $|N_{G^F}(S)/C_{G^F}(S)|$.

Parabolic subgroups and Levis

A group P containing a Borel subgroup is a parabolic subgroup.
It has a *Levi decomposition* $P = V \rtimes L$ where V is its unipotent radical, and L is a reductive group; L is what is called a Levi subgroup of G.
Example: For GL_n upper block-triangular matrices are the parabolic subgroup containing the Borel of upper triangular matrices. The corresponding Levi is block-diagonal.

The centralizer of a torus is a Levi subgroup, thus if S is a Φ_d-Sylow, $L := C_G(S)$ is a Levi subgroup. We have $W_G(L) = N_G(L)/L = N_G(S)/C_G(S)$; this "relative Weyl group" is such that $W_G(L)^F$ is a complex reflection group. As for a torus, L is the connected component of $N_G(L)$; we have $C_G(S) = N_G(S)^0$.

If S corresponds to a maximal ζ_d-eigenspace U of some element of WF, the Levi $L = C_G(S)$ has weyl group $C_W(U)$.

ℓ-Sylows and Φ_d-Sylows

Assume that the ℓ-Sylow S_ℓ of G^F is abelian. Then $|S_\ell|$ divides a unique factor $\Phi_d(q)^{|a(d)|}$ of G^F, and there is a unique Φ_d-Sylow S such that $S_\ell \subset S$.

It follows that

- $C_{\mathbf{G}}(S) = C_{\mathbf{G}}(S_\ell)$ is a Levi subgroup.
- $N_{G^F}(S_\ell)/C_{G^F}(S_\ell) = N_{G^F}(S)/C_{G^F}(S)$ is a complex reflection group.