Group Actions and Finite Fields

Daniel Litt

February 9, 2011

1 Introduction

The goal of this note is to give some elementary techniques for understanding linear algebraic groups over finite fields, and the sets on which they act, with an aim towards solving problems on the Stanford Algebra Quals. There will be some exercises, which, while not necessarily easy, can be done in your head, and in any case some exercises will be solved later on in the note.

By an algebraic group, I will mean a subgroup of the group

$$GL_n(\mathbb{F}_q) \text{ with } n > 0, q \text{ a prime power.}$$

Of course any finite group is such a group if n is taken large enough, as G embeds in $GL_{|G|}(\mathbb{F}_q)$ for any q via permutation matrices. So we will focus on groups cut out by a single polynomial equation (such as $\det(A) = 1$) or quotients thereof.

Example 1 (The General Linear Group)**.** *$GL_n(\mathbb{F}_q)$ consists of those $n \times n$ matrices with entries in $\mathbb{F}_q$ whose entries are invertible.*

Example 2 (The Special Linear Group)**.** *$SL_n(\mathbb{F}_q) \subset GL_n(\mathbb{F}_q)$ consists of those matrices with entries in $\mathbb{F}_q$ with determinant 1.*

Example 3 (Projective Groups)**.** *$PGL_n(\mathbb{F}_q)$ is the quotient of $GL_n(\mathbb{F}_q)$ by its center, the scalar matrices. $PSL_n(\mathbb{F}_q)$ is the quotient of $SL_n(\mathbb{F}_q)$ by its center, which again consists of scalar matrices.*

Exercise 1. *Show that the centers of $GL_n(\mathbb{F}_q), SL_n(\mathbb{F}_q)$ consist exactly of the scalar matrices. Which scalar matrices are in $SL_n(\mathbb{F}_q)$?*

There are several spaces that are commonly acted upon by such groups. Most obviously, any subgroup of $GL_n(\mathbb{F}_q)$ acts on the vector space $\mathbb{F}_q^n$, via linear transformations. But more generally, all of the groups mentioned in examples $1-3$ act on the following type of space:

Example 4 (Flag Varieties)**.** *Let V be a vector space over $\mathbb{F}_q$ of dimension n, and fix an integer $k < n$ and integers $0 < i_1 < i_2 < \cdots < i_k < n$. Then as a set, we have*

$$\mathrm{Fl}_{i_1,\ldots,i_k}(V) = \{\textit{subspaces } 0 \subset V_1 \subset V_2 \subset \cdots V_n \subset V \textit{ such that } \dim(V_j) = i_j \textit{ for all } 1 \leq j \leq k\}.$$

In words, the flag variety consists of nested sequences of vector subspaces with specified dimensions. The flag variety has additional structure—it has a topology, for example—but that won't be relevant to our purposes.

There are several important examples of flag varieties, which you've likely run into in the past. $\mathrm{Fl}_r(V)$ is the Grassmannian of r-planes in V, $\mathrm{Gr}(r, V)$—namely, its points correspond to r dimensional subspaces of V. If $r = 1$, we have $\mathrm{Fl}_q(V) = \mathrm{Gr}(1, V) = \mathbb{P}(V)$, the projectivization of V, whose points are one-dimensional subspaces, or lines, in V.

$GL_n(\mathbb{F}_q)$ and $SL_n(\mathbb{F}_q)$ act on the flag varieties through linear transformations; it should be clear that scalar matrices act trivially, inducing actions by PGL_n and PSL_n.

Exercise 2. *Let V be a two-dimensional vector space over $\mathbb{F}_q$. How many points are in $\mathbb{P}(V)$?*

Exercise 3 (Important!)**.** *Check that the action $PSL_n(\mathbb{F}_q)$ on $\mathrm{Fl}_{1,2,\ldots,n-1}(\mathbb{F}_q^n)$ is transitive. Note that this implies the action of all the groups we've mentioned on every flag variety we've mentioned is transitive. Fix your favorite point $x \in \mathrm{Fl}_{1,2,\ldots,n-1}(\mathbb{F}_q)^n$ and find its stabilizer in $GL_n(\mathbb{F}_q)$.*

2 Counting Points

One common problem involves counting points, either in linear algebraic groups, or in flag varieties. The two important propositions here are both trivial and awesome.

Proposition 1. *Let G be a group acting transitively on a set X. Let $x \in X$ be any element, and let S be the stabilizer of x in G. Then there is a "natural" isomorphism $G/S \xrightarrow{\sim} X$.*

Proof. We define the map $f : G/S \to X$ as $f(gS) = gx$. This is well-defined, as if $gS = g'S$, then $g' = gs$ for some $s \in S$, and thus $g'x = gsx = gx$.

Exercise 4. *Check that f is bijective.*

□

Proposition 2. *Let G, X be as above, and let $x, x' \in X$ be two elements. Let S, S' be the stabilizers of x, x', respectively. Then S and S' are conjugate subgroups in G.*

Proof. As G acts transitively on X, there exists $g \in G$ with $gx = x'$. Then given $s \in S$, we have that

$$gsg^{-1}x' = gsx = gx = x',$$

and thus $gSg^{-1} \subset S'$. Similarly, $g^{-1}Sg \subset S$, so g conjugates S to S'. □

We'll now do some direct calculations.

Proposition 3. *The number of points in $GL_n(\mathbb{F}_q)$ is*

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

More generally, the number of full rank $k \times n$ matrices, $0 \le k < n$, with elements in $\mathbb{F}_q$ is

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}).$$

Proof. An element of $GL_n(\mathbb{F}_q)$ is the same as an ordered collection $(e_1, ..., e_n)$ of vectors in $\mathbb{F}_q^n$, such that the e_i are linearly independent. We will compute, by induction, the number of ordered collections $(e_1, e_2, ..., e_k)$ of linearly independent vectors in $\mathbb{F}_q^n$ for $k < n$. For $k = 0$, there is clearly one such collection—the empty collection. Assume as the inductive step that there are

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})$$

such collections of k vectors. Then we may choose our $k + 1$-th vector to be any vector not in the span of $e_1, ..., e_k$. This span is a k-dimensional vector space by linear independence, and thus contains q^k elements, so its complement in $\mathbb{F}_q^n$ contains $q^n - q^k$ elements. Thus there are

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})(q^n - q^k)$$

collections of $k - 1$ linearly independent vectors.

Taking $k = n$ gives the first statement. □

We'll now very rapidly do an old qual problem, using propositions 1 and 3 above.

Proposition 4. *The number of points in* $\mathrm{Gr}(k, \mathbb{F}_q^n)$ *is*

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

Proof. The strategy will be to find a group acting transitively on the space in question, and then find the size of the stabilizer of some point. This will allow us to apply Proposition 1 above.

By basic linear algebra, the group $GL_n(\mathbb{F}_q)$ acts transitively on $\mathrm{Gr}(k, \mathbb{F}_q^n)$ via linear transformations. Let $V \subset \mathbb{F}_q^n$ be the k-dimensional subspace spanned by $e_1, e_2, ..., e_k$, the first k standard basis elements of $\mathbb{F}_q^n$. Then the stabilizer of V consists of those invertible matrices of the form

$$\begin{pmatrix} A_{k\times k} & B_{k\times(n-k)} \\ 0 & C_{(n-k)\times(n-k)} \end{pmatrix}$$

where the subscripts indicate the size of the block matrix. $A_{k\times k}$ may be any element of $GL_k(\mathbb{F}_q)$; the rightmost $n-k$ columns of such a matrix may be any $n-k$ linearly vectors completing the columns of $A_{k\times k}$ to a basis of $\mathbb{F}_q^n$; as before, there are

$$(q^n-q^k)(q^n-q^{k+1})\cdots(q^n-q^{n-1})$$

options. Putting this together with proposition 3, the stabilizer S of V has size

$$\left((q^k-1)(q^k-q)\cdots(q^k-q^{k-1})\right)\left((q^n-q^k)(q^n-q^{k+1})\cdots(q^n-q^{n-1})\right).$$

But by Proposition 1, $\mathrm{Gr}(k, \mathbb{F}_q^n) \simeq GL_n(\mathbb{F}_q)/S$, and thus dividing the numbers we've computed gives the proof. □

Remark 1 (On Simplifying Answers)**.** *A common way to simplify the ridiculous expressions one obtains in these sorts of problems is as follows. Namely, define*

$$[n]_q = \frac{q^n-1}{q-1} = 1+q+q^2+\cdots+q^{n-1}$$

and let

$$[n]_q! = [n]_q[n-1]_q[n-2]_q\cdots[1]_q$$

and

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}.$$

Note that as $q \to 1$, $[n]_q \to n$, *and thus* $[n]_q! \to n!$, *and* $\binom{n}{k}_q \to \binom{n}{k}$, *which perhaps should justify the notation. Now you can check that we've shown that*

$$\#GL_n(\mathbb{F}_q) = [n]_q!(q-1)^n q^{\binom{n}{2}}$$

(note that Wikipedia has an error here!) and

$$\#\,\mathrm{Gr}(k, \mathbb{F}_q^n) = \binom{n}{k}_q.$$

So if you'd like, you can think of $GL_n(\mathbb{F}_q)$ *as the analogue of* S_n *over the finite field* $\mathbb{F}_q$*, and perhaps more convincingly, you can think of* $\mathrm{Gr}(k, \mathbb{F}_q^n)$ *as being analogous to the collection of* k*-element subsets of a set of size* n*. And indeed, if you carefully look at the proof that the binomial coefficient counts elements of this latter collection, you'll see that it is essentially identical to the proof of Proposition* 4*.*

Exercise 5. *Use this method to compute the number of points in some other flag variety; for example, if you've done Exercise* 3*, counting points in* $\mathrm{Fl}_{1,2,...,n-1}(\mathbb{F}_q^n)$ *should be no trouble.*

3 Analyzing Group Structure

We'll first consider the case $n = 1$. You've probably seen the following result, but I'll include a proof for completeness.

Proposition 5. *$GL_1(\mathbb{F}_q) \simeq \mathbb{F}_q^\times$ is cyclic of order $q-1$.*

Proof. I first claim that $m := \mathrm{lcm}_{x\in\mathbb{F}_q^\times} |x| = q-1$, where by $|x|$ I mean the multiplicative order of x. Indeed, $x^{q-1} = 1$ for any $x \in \mathbb{F}_q^\times$, as $\#\mathbb{F}_q^\times = q-1$, so $|x|$ divides $q-1$ for all x. Thus $m \leq q-1$.

But the polynomial $x^m - 1$ vanishes for each $x \in \mathbb{F}_q^\times$, and thus has $q-1$ zeros, so $m \geq q-1$ (as the degree of a polynomial over a field is bounded below by the number of zeros it has).

Now

$$\mathbb{F}_q^\times = \prod_{p \text{ prime}} C_p,$$

where C_p is an Abelian p-group; it suffices to show each C_p is cyclic. But letting $m_p = \max_{x\in C_p} |x|$, we have that

$$\prod_{p \text{ prime}} \#C_p = \#\mathbb{F}_q^\times = q-1 = \mathrm{lcm}_{x\in\mathbb{F}_q^\times} |x| = \prod_{p \text{ prime}} m_p.$$

Thus by unique prime factorization, $m_p = \#C_p$, and so each C_p is cyclic as desired. □

This result, as long as various tricks with counting and group action, will be the most important tool we use in analyzing the structure of our linear algebraic groups.

We now are able to do (a bit of a strengthening) of another old qual problem:

Proposition 6. *Let G be the group $SL_2(\mathbb{F}_q)$. Then if p is an odd prime, the p-Sylow subgroup of G is cyclic, unless $p \mid q$. In this case, (even if $p = 2$), the p-Sylow subgroup is isomorphic to the additive group of $\mathbb{F}_q$ (in particular, if $q = p^k$, then it is $(\mathbb{Z}/p\mathbb{Z})^k$).*

Proof. We first compute the order of G. G is the kernel of the determinant map

$$\det : GL_2(\mathbb{F}_q) \to \mathbb{F}_q^\times,$$

which is surjective, and thus the kernel has order

$$\#SL_2(\mathbb{F}_q) = \#GL_2(\mathbb{F}_q)/\#\mathbb{F}_q^\times = (q^2-1)(q^2-q)/(q-1) = (q-1)q(q+1).$$

If p is an odd prime, it divides at most one of $q-1, q$, and $q+1$. We do each case separately.

Case 1: $(p \mid q-1)$. It suffices to show that $SL_2(\mathbb{F}_q)$ contains a cyclic group of order $q-1$. But matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

for $a \in \mathbb{F}_q^\times$ suffice, and this subgroup is cyclic as it is isomorphic to $\mathbb{F}_q^\times$.

Case 2: $(p \mid q)$ This argument works even if p is even, as then it divides neither $q-1, q+1$. Consider matrices of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

for $b \in \mathbb{F}_q$. Then matrices of this form are isomorphic to the additive group $\mathbb{F}_q$, giving the desired claim.

Case 3: $(p \mid q+1)$ It suffices to show that G contains a cyclic subgroup of order $q+1$.

This is the trickiest part. Consider the field $\mathbb{F}_{q^2}$, which is a two-dimensional vector space over $\mathbb{F}_q$. Then picking a basis of this vector space induces a natural inclusion $\mathbb{F}_{q^2}^\times \hookrightarrow GL_2(\mathbb{F}_q)$ (we identify an element of $\mathbb{F}_{q^2}^\times$ with the linear map corresponding to its action by multiplication on the two-dimensional vector space $\mathbb{F}_{q^2}$).

The elements of $\mathbb{F}_{q^2}^\times$ that land in G via this inclusion are those elements g such that multiplication by g is a linear map of determinant 1; namely, exactly those elements g of $\mathbb{F}_{q^2}^\times$ with $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = 1$. We claim that there are exactly $q+1$ such elements. Indeed, the norm map $\mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$ is surjective, so the kernel has size $(q^2-1)/(q-1) = q+1$.

But then the norm 1 elements of $\mathbb{F}_{q^2}^\times$ give a subgroup of G of size $q+1$; but they are a subgroup of $\mathbb{F}_{q^2}^\times$, which is cyclic, completing the proof. □

Case 3 above seems like a trick; I claim it's really part of a more general technique. Say we are interested in the group $GL_n(\mathbb{F}_q)$ or some subquotient thereof. Often we have direct access to some large subgroup of $GL_n(\mathbb{F}_q)$ as follows:

Proposition 7. *There is a natural map $\phi : \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Aut}(\mathbb{F}_{q^n}^\times)$. Choosing a basis for $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$ induces an inclusion*

$$\mathbb{F}_{q^n}^\times \rtimes_\phi \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to GL_n(\mathbb{F}_q).$$

Proof. Having chosen a basis, left multiplication by an element of $\mathbb{F}_{q^n}$ has a matrix form, as does the action by $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$; this gives a map of sets. I'll leave checking that this is an injective homomorphism as an exercise—it's a tiny bit tricky, and worth doing yourself. Note that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ acts on $\mathbb{F}_{q^n}^\times$ by *conjugation.* □

As an example, we'll compute the structure of the 2-Sylow subgroup of $GL_2(\mathbb{F}_7)$, another old qual problem.

Proposition 8. *The 2-Sylow subgroup of $GL_2(\mathbb{F}_7)$ has presentation*

$$\langle x, g \mid g^2 = x^{16} = e,\ gxg^{-1} = x^7 \rangle.$$

Proof. Note that $\#GL_2(\mathbb{F}_7) = (7^2-1)(7^2-7) = 48 \cdot 42$, and thus its 2-Sylow subgroup has order 32. Now consider the subgroup given by proposition 7 above, namely $H := \mathbb{F}_{49}^\times \rtimes_\phi \mathrm{Gal}(\mathbb{F}_{49}/\mathbb{F}_7)$. As $\mathrm{Gal}(\mathbb{F}_{49}/\mathbb{F}_7) = \mathbb{Z}/2\mathbb{Z}$, this group has order $48 \cdot 2$, and thus also as 2-Sylow subgroup of order 32. Thus it suffices to find the structure of the 2-Sylow subgroup of H.

H itself is a semidirect product of $\mathbb{Z}/48\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, so the 2-Sylow subgroup in question is a semidirect product of $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$; we must only determine which homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/16\mathbb{Z})$ induces the semidirect product.

We may write $\mathbb{F}_{49} = \mathbb{F}_7[\sqrt{-1}]$, as it is the unique quadratic extension of $\mathbb{F}_7$. Choose the basis $\{1, \sqrt{-1}\}$. Then $x = 2 + 3\sqrt{-1}$ is a primitive 16-th root of unity in $\mathbb{F}_{49}$, and the nontrivial element of the Galois group action sends it to $g(x) = 2 - 3\sqrt{-1} = x^7$. As the action of $\mathrm{Gal}(\mathbb{F}_{49}/\mathbb{F}_7)$ on $\mathbb{F}_{49}^\times$ in H is given by conjugation, this completes the proof. □

Finally we'll do a problem involving a bit more of the structure of these groups, combining a lot of what we've done before. This is a problem from the Fall 2010 Quals.

Proposition 9. *Let $G = GL_2(\mathbb{F}_q)$, where $q = p^n$. Given three distinct p-Sylow subgroups P_1, P_2, P_3, and three distinct p-Sylow subgroups Q_1, Q_2, Q_3, there exists $g \in G$ such that*

$$gP_1g^{-1} = Q_1, gP_2g^{-1} = Q_2, gP_3g^{-1} = Q_3.$$

That is, G acts triply transitively (by conjugation) on its p-Sylow subgroups.

Proof. We first do a bit of counting. We have that

$$\#G = (q^2-1)(q^2-q) = (q-1)^2(q+1)q.$$

As p does not divide $q-1, q+1$, the p-Sylow subgroups each have order q.

Now consider the action of G on $\mathbb{P}^1(\mathbb{F}_q)$, the set of one-dimensional subspaces of $\mathbb{F}_q^2$, which has size $q+1$. As G acts transitively on $\mathbb{P}^1(\mathbb{F}_q)$, the stabilizer of a line $S(\ell)$ has order $(q-1)^2q$; we claim that the stabilizer of each line contains a unique p-Sylow subgroup (which by counting is then a p-Sylow subgroup of G).

It suffices to check this for a single line ℓ; consider the line spanned by $(1,0)$. Then the stabilizer $S(\ell)$ consists of matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

with a and c both nonzero. The a p-Sylow subgroup is by inspection matrices of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

One may check directly that this is a normal subgroup of $S(\ell)$, giving uniqueness. (For example, by noting that conjugation by upper triangular matrices preserves the property of being upper triangular, and that conjugation preserves eigenvalues.)

So we have that p-Sylow subgroups are in bijection with elements of $\mathbb{P}^1(\mathbb{F}_q)$, via sending a line to the unique p subgroup in its stabilizer; by Proposition 2, it suffices to show that G acts triply transitively on $\mathbb{P}^1(\mathbb{F}_q)$. Indeed, we show that given distinct lines ℓ_1, ℓ_2, ℓ_3, we may send the spans of $(1,0)$, $(0,1)$, and $(1,1)$ to ℓ_1, ℓ_2, ℓ_3 respectively. Let ℓ_i be spanned by v_i; we may write $v_3 = av_1 + bv_2$, as v_1, v_2 are linearly independent and thus form a basis.

Now let $T \in G$ be the linear transformation such that

$$T(1,0) = av_1, T(0,1) = bv_2,$$

and extending by linearity. Then by inspection, $T(\text{Span}(1,0)) = \ell_1, T(\text{Span}(0,1)) = \ell_2, T(\text{Span}(1,1)) = \ell_3$, and thus we have triple transitivity as desired. □