Grassmann varieties

Definition 1. Suppose that $F$ is a field, $n$ is a non-negative integer, and $F^n$ is the standard $n$-dimensional vector space consisting of $n$-tuples of elements of $F$. For us it will generally be best to regard $F^n$ as consisting of $n \times 1$ column vectors, so that $n \times n$ matrices can act on the left by matrix multiplication. The Grassmann variety $G(k, n)(F)$ of $k$-planes in $F^n$ is the set of all $k$-dimensional vector subspaces of $F^n$. This set is non-empty for integers $k$ between 0 and $n$: $0 \leq k \leq n$.

Recall that $G = GL(n, F)$ is the group of invertible $n \times n$ matrices with entries in $F$. There is an action of $G$ on the Grassmann variety $G(k, n)(F)$, defined as follows. Suppose that $V$ is a $k$-dimensional subspace of $F^n$, so that $V \in G(k, n)(F)$. We define a new $k$-dimensional subspace $g \cdot V$ of $F^n$ by

$$g \cdot V = \{g \cdot v \mid v \in V\}.$$  

That is, we apply the matrix $g$ to each of the vectors in $V$. It’s very easy to check that $g \cdot V$ is indeed a $k$-dimensional subspace, and that this is an action of $G$ on the Grassmann variety.

The Grassmann varieties (“Grassmannians” for short) are fundamental to all kinds of mathematics. When the field $F$ is $\mathbb{R}$ or $\mathbb{C}$, $G(k, n)(F)$ is a manifold; it turns out to be a compact manifold of dimension $k(n - k)$ (if $F = \mathbb{R}$) or $2k(n - k)$ (if $F = \mathbb{C}$). For arbitrary fields, the Grassmann variety consists of the “$F$-points” of a smooth algebraic variety of dimension $k(n - k)$.

Today I want to concentrate on counting points in a Grassmann variety over a finite field, and what that has to do with $GL(n)$.

There is one obvious $k$-dimensional subspace of $F^n$: the collection of vectors whose last $n - k$ coordinates are all zero. This subspace has a natural identification with $F^k$, and I’ll write it as $F^k \subset F^n$. If $g \in GL(n, F)$, then

(1) $$g \cdot F^k = \text{span} \text{ of the first } k \text{ columns of } g.$$  

Now the first $k$ columns of a matrix in $GL(n, F)$ can be any $k$ linearly independent vectors. (The reason is that any set of $k$ independent vectors can be enlarged to a basis of $F^n$; and the bases of $F^n$ are precisely the sets of columns of invertible matrices.) In the language of group actions, this means

$$GL(n, F) \cdot F^k = G(k, n)(F).$$  

That is, the Grassmann variety is a single orbit of $GL(n, F)$. (The mathematical word is transitive: the action of $GL(n, F)$ on $G(k, n)(F)$ is transitive.)

Because of this fact, it is interesting to understand the isotropy group

(2) $$GL(n, F)_{F^k} = \{g \in GL(n, F) \mid g \cdot F^k = F^k\}.$$
Proposition 1. Suppose $0 \leq k \leq n$ are integers. Then the isotropy group at $F^k$ for the action of $GL(n, F)$ on the Grassmann variety $G(k, n)(F)$ is

$$GL(n, F)_{F^k} = \left\{ g = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \mid A \in GL(k, F), \\
C \in GL(n-k, F), \ B \in M(k \times (n-k), F) \right\}.$$

Here $M(p \times q, F)$ is the collection of all $p \times q$ matrices with entries in $F$, and $0$ is the $(n-k) \times k$ zero matrix.

Proof. Because $g \cdot F^k$ is a $k$-dimensional subspace of $F^n$ (for any $g \in GL(n, F)$), it is equal to $F^k$ if and only if it is contained in $F^k$. We may therefore rewrite (2) as

$$GL(n, F)_{F^k} = \{ g \in GL(n, F) \mid g \cdot F^k \subset F^k \}.$$

A vector $v \in F^n$ belongs to $F^k$ if and only if its last $n-k$ coordinates are zero. In light of (1), we may therefore write (3) as

$$GL(n, F)_{F^k} = \left\{ g \in GL(n, F) \mid g = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}, A \in M(k \times k, F), \\
C \in M((n-k) \times (n-k), F), \ B \in M(k \times (n-k), F) \right\}.$$

For a matrix $g$ as in (4), $\det g = (\det A)(\det C)$; so $g$ belongs to $GL(n, F)$ if and only if both $A \in GL(k, F)$ and $C \in GL(n-k, F)$. □

Proposition 2. Suppose $\mathbb{F}_q$ is a finite field with $q$ elements. Then

$$|GL(n, \mathbb{F}_q)| = |G(k, n)(\mathbb{F}_q)| \cdot |GL(n, \mathbb{F}_q)_{F^k}|$$

$$= |G(k, n)(\mathbb{F}_q)| \cdot |GL(k, \mathbb{F}_q)| \cdot q^{k(n-k)} \cdot |GL(n-k, \mathbb{F}_q)|.$$

Equivalently,

$$|G(k, n)(\mathbb{F}_q)| = \frac{|GL(n, \mathbb{F}_q)|}{q^{k(n-k)} \cdot |GL(k, \mathbb{F}_q)| \cdot |GL(n-k, \mathbb{F}_q)|}.$$

The last three factors in the second formula count the elements of $GL(n, \mathbb{F}_q)_{F^k}$, as described in Proposition 1; they are the number of choices for the matrices $A$, $B$, and $C$ respectively. The entire formula is therefore our basic formula for counting points in an orbit of a group action.

Last week Gabe Cunningham proved a formula for the number of elements in the general linear group over a finite field:

$$|GL(n, \mathbb{F}_q)| = q^{n(n-1)/2} \prod_{k=1}^{n} (q^k - 1).$$

It’s often useful to rewrite this a bit, by removing the common factor of $q-1$ from each of the last $n$ factors:

$$|GL(n, \mathbb{F}_q)| = q^{n(n-1)/2} (q - q^n) \prod_{k=1}^{n} \frac{q^k - 1}{q - 1}$$

$$= q^{n(n-1)/2} (q - 1)^n \prod_{k=1}^{n} (q^{k-1} + q^{k-2} + \cdots + 1).$$
Definition 2. Suppose \( f \) is a function taking integer values. (I haven’t specified the domain; often it’s the non-negative integers, but anything is allowed.) Explicitly, \( f : X \to \mathbb{Z} \).

A \( q \)-analogue of \( f \) is a function

\[
f_q : S \to \mathbb{Z}[q]
\]

taking values in polynomials in \( q \), with the property that \( f_1 = f \); that is, that the value at \( q = 1 \) of the polynomial \( f_q(s) \) is equal to the integer \( f(s) \).

It’s clear that a \( q \)-analogue of \( f \) is not unique. (There is always a stupid \( q \)-analogue, in which \( f_q(s) \) is the constant polynomial \( f(s) \).) But some \( q \)-analogues arise often enough to have names of their own; they’re called “the” \( q \)-analogue, even though there are others. The \( q \)-analogue of \( n \) (defined for every non-negative integer \( n \)) is

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

We use the convention that an empty sum is zero, so

\[
[0]_q = 0, \\
[1]_q = 1, \\
[2]_q = q + 1, \\
[3]_q = q^2 + q + 1.
\]

The \( q \)-analogue of \( n! \) (defined for every non-negative \( n \)) is

\[
[n!]_q = \prod_{k=1}^{n} [n]_q = \prod_{k=1}^{n} \frac{q^n - 1}{q - 1}.
\]

We use the convention that an empty product is 1 (why is that reasonable?), so that \([0!]_q = 1\). For example,

\[
[3!]_q = 1(q + 1)(q^2 + q + 1) = q^3 + 2q^2 + 2q + 1.
\]

Using these factorials, we can formally define the \( q \)-analogue of \( \binom{n}{k} \) as

\[
\binom{n}{k}_q = \frac{[n!]_q}{[k!]_q \cdot [(n-k)!]_q}.
\]

It isn’t clear from this definition that this function of \( n \) and \( q \) is actually a polynomial (with integer coefficients) in \( q \). We’ll see that eventually. One reason that this definition is interesting is Proposition 4 below.

You can read much more about \( q \)-analogues in Quantum Calculus, by Victor Kac and Pokman Cheung.
Using Definition 2, we can rewrite the formula (6) for the cardinality of $GL(n, \mathbb{F}_q)$ as

\begin{equation}
|GL(n, \mathbb{F}_q)| = q^{n(n-1)/2}(q-1)^n[n!]_q.
\end{equation}

This is a $q$-analogue of 1, times a $q$-analogue of 0, times “the” $q$-analogue of $n!$. By ignoring the zero part, we get a really important metamathematical idea:

\begin{equation}
GL(n, \mathbb{F}_q) \text{ is a } q\text{-analogue of the symmetric group } S_n.
\end{equation}

This isn’t mathematics: there’s no definition of a $q$-analogue of a group along the lines of Definition 2. But it’s a useful idea to keep in mind. Ideas that tell you something about $GL(n, \mathbb{F}_q)$ may often tell you something about $S_n$, and vice versa.

Now we can plug (7) (three times, for $n$ and $k$ and $n-k$) into the second formula of Proposition 2, and get

**Proposition 3.** Suppose $\mathbb{F}_q$ is a finite field with $q$ elements. Then

\[ |G(k, n)(\mathbb{F}_q)| = \frac{[n]_q}{[k]_q[k](n-k)!}_q = \left[ \begin{array}{c} n \\ k \end{array} \right]_q. \]

That is, the number of $k$-dimensional subspaces of $\mathbb{F}_q^n$ is equal to the $q$-binomial coefficient $\left[ \begin{array}{c} n \\ k \end{array} \right]_q$.

To prove this, one has to check that the powers of $(q - 1)$ all cancel (easy), and that the powers of $q$ all cancel (straightforward but not quite as easy; I usually have to do it a couple of times before I get the signs right). I’ll omit the details.

The metamathematical idea here is

\begin{equation}
G(k, n)(\mathbb{F}_q) \text{ is a } q\text{-analogue of } k\text{-element subsets of } \{1, \ldots, n\}.
\end{equation}

This statement has a bit more concrete content than (8): the cardinality of the first set is indeed a $q$-analogue of the cardinality of the second, according to Proposition 3.

There are many cheerful facts about binomial coefficients, and many of these facts have $q$-analogues. Here is the most fundamental.

**Proposition 4.** Suppose $0 < k < n$ are strictly positive integers. Then

\[
\left[ \begin{array}{c} n \\ k \end{array} \right]_q = q^{n-k} \left[ \begin{array}{c} n-1 \\ k-1 \end{array} \right]_q + \left[ \begin{array}{c} n-1 \\ k \end{array} \right]_q
\]

\[ = \left[ \begin{array}{c} n-1 \\ k-1 \end{array} \right]_q + q^k \left[ \begin{array}{c} n-1 \\ k \end{array} \right]_q.
\]

Notice that the two formulas here are not the same when $q$ is not 1. If I get ambitious I’ll prove this formula in the seminar on Tuesday, but I’m too lazy to write the proof here.

The formula in Proposition 4 implies (by induction on $n$) that the $q$-binomial coefficient is indeed a polynomial in $q$, with non-negative integer coefficients. The next Proposition more or less gives an interpretation for the coefficients: it says that they solve a certain counting problem.
Proposition 4. Suppose $0 \leq k \leq n$ are non-negative integers. Write

$$N = \{1, 2, \ldots, n\}.$$ 

Fix a $k$-element subset

$$S = \{i_1 < i_2 < \cdots < i_k\} \subset N.$$

We attach to $S$ a non-negative integer

$$l(S) = \sum_{j=1}^{k} \text{number of elements of } N - S \text{ strictly larger than } i_k.$$ 

(1) We have $l(S) \leq k(n - k)$, with equality if and only if $S = \{1, 2, \ldots, k\}$.

(2) We have $l(S) \geq 0$, with equality if and only if $S = \{n-k+1, n-k+2, \ldots, n\}$.

(3) The $q$-binomial coefficient satisfies

$$\binom{n}{k}_q = \sum_{S \subset N, |S| = k} q^{l(S)}.$$ 

Consequently the $q$-binomial coefficient is a polynomial with non-negative coefficients, of degree $k(n - k)$, with constant and leading coefficients both equal to 1.

You should be able to see (1) and (2) pretty easily; the tricky part is (3). Again I’ll hope to prove this in the seminar.