18.704 Gabe Cunningham
2/18/05 gcasey@mit.edu

The General Linear Group

Definition: Let F be a field. Then the *general linear group* $GL_n(F)$ is the group of invertible $n \times n$ matrices with entries in F under matrix multiplication.

It is easy to see that $GL_n(F)$ is, in fact, a group: matrix multiplication is associative; the identity element is I_n, the $n \times n$ matrix with 1's along the main diagonal and 0's everywhere else; and the matrices are invertible by choice. It's not immediately clear whether $GL_n(F)$ has infinitely many elements when F does. However, such is the case. Let $a \in F$, $a \neq 0$. Then $a \cdot I_n$ is an invertible $n \times n$ matrix with inverse $a^{-1} \cdot I_n$. In fact, the set of all such matrices forms a subgroup of $GL_n(F)$ that is isomorphic to $F^\times = F \setminus \{0\}$.

It is clear that if F is a finite field, then $GL_n(F)$ has only finitely many elements. An interesting question to ask is how many elements it has. Before addressing that question fully, let's look at some examples.

Example 1: Let $n = 1$. Then $GL_n(\mathbb{F}_q) \cong \mathbb{F}_q^\times$, which has $q - 1$ elements.

Example 2: Let $n = 2$; let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then for M to be invertible, it is necessary and sufficient that $ad \neq bc$. If a, b, c, and d are all nonzero, then we can fix a, b, and c arbitrarily, and d can be anything but $a^{-1}bc$. This gives us $(q-1)^3(q-2)$ matrices. If exactly one of the entries is 0, then the other three entries can be anything nonzero, for a total of $4(q-1)^3$ matrices. Finally, if exactly two entries are 0, then these entries must be opposite each other for the matrix to be invertible, and the other two entries can be anything nonzero, for a total of $2(q-1)^2$ matrices. So that gives us

$$\begin{aligned}
&(q-1)^3(q-2) + 4(q-1)^3 + 2(q-1)^2 \\
&= (q-1)^2\left[(q-1)(q-2) + 4(q-1) + 2\right] \\
&= (q-1)^2[q^2 + q] \\
&= (q^2 - 1)(q^2 - q)
\end{aligned}$$

In general, calculating the size of $GL_n(\mathbb{F}_q)$ by directly calculating the determinant, then determining what values of the entries make the determinant nonzero, is tedious and error-prone. Thankfully, there's an easier way to determine whether a matrix is invertible. One of the basic properties of determinants is that the determinant of a matrix is nonzero if and only if the rows of the matrix are linearly independent. Armed with this result, we're ready to determine how many elements $GL_n(\mathbb{F}_q)$ has.

Proposition 1: The number of elements in $GL_n(\mathbb{F}_q)$ is $\prod_{k=0}^{n-1}(q^n - q^k)$.
Proof: We will count the $n \times n$ matrices whose rows are linearly independent. We do so by building up a matrix from scratch. The first row can be anything other than the zero row, so there are $q^n - 1$ possibilities. The second row must be linearly independent from the first, which is to say that it must not be a multiple of the first. Since there are q multiples of the first row, there are $q^n - q$ possibilities for the second row. In general, the i^{th} row must be linearly independent from the first $i-1$ rows, which means that it can't be a linear combination of the first $i-1$ rows. There are q^{i-1} linear combinations of the first $i-1$ rows, so there are $q^n - q^{i-1}$ possibilities for the i^{th} row. Once we build the entire matrix this way, we know that the rows are all linearly independent by choice. Also, we can build any $n \times n$ matrix whose rows are linearly independent in this fashion. Thus, there are $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = \prod_{k=0}^{n-1}(q^n - q^k)$ matrices.

Now we'll consider an interesting subgroup of $GL_n(F)$. The determinant function, $det : GL_n(F) \to F^\times$ is a homomorphism; it maps the identity matrix to 1, and it is multiplicative, as desired. We define the *special linear group*, $SL_n(F)$, to be the kernel of this homomorphism. Put another way, $SL_n(F) = \{M \in GL_n(F) \mid det(M) = 1\}$.

Proposition 2: The number of elements in $SL_n(\mathbb{F}_q)$ is $\left(\prod_{k=0}^{n-1}(q^n - q^k)\right) \backslash (q-1)$.
Proof: Consider the homomorphism $det : GL_n(F) \to F^\times$. This map is surjective; that is, the image of $GL_n(F)$ under det is the whole space $F^\times$. This is true because, for instance, the matrix

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

is an invertible $n \times n$ matrix of determinant a. Since $SL_n(\mathbb{F}_q)$ is the kernel of the homomorphism, it follows from the First Isomorphism Theorem that $GL_n(\mathbb{F}_q) \backslash SL_n(\mathbb{F}_q) \cong F^\times$. Therefore,

$$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{|F^\times|} = \frac{\prod_{k=0}^{n-1}(q^n - q^k)}{q-1}$$

Now, in order to talk about two more subgroups of $GL_n(F)$, we need to define the notion of the center of a group.

Definition: The *center* of a group G, denoted $Z(G)$, is the set of $h \in G$ such that $\forall g \in G,\ gh = hg$.

Proposition 3: $Z(G)$ is a subgroup of G.
Proof: 1 is in $Z(G)$ because $\forall g \in G, 1 \cdot g = g \cdot 1 = g$. Let $h_1, h_2 \in Z(G)$. Then $\forall g \in G$,

$$h_1 h_2 g = h_1(h_2 g) = h_1(g h_2) = (h_1 g)h_2 = g h_1 h_2,$$

so $h_1 h_2 \in Z(G)$. Finally, if $h \in Z(G)$, then $\forall g \in G$,

$$\begin{aligned} hg &= gh \\ h^{-1}hgh^{-1} &= h^{-1}ghh^{-1} \\ gh^{-1} &= h^{-1}g \end{aligned}$$

so $h^{-1} \in Z(G)$.

Now let's look at the centers of $GL_n(F)$ and $SL_n(F)$.

Proposition 4: $Z(GL_n(F)) = \{a \cdot I_n \mid a \in F^\times\}$; $Z(SL_n(F)) = \{a \cdot I_n \mid a \in F^\times, a^n = 1\}$
Proof idea: For M to be in $Z(GL_n(F))$, it must commute with every $N \in G$. In particular, M commutes with the elementary matrices. Multiplying M on the left by an elementary matrix corresponds to performing an elementary row operation; multiplying M on the right by an elementary matrix corresponds to performing an elementary column operation. So, for instance, multiplying the i^{th} row of M by a gives you the same matrix as multiplying the i^{th} column of M by a. This implies that the matrix is diagonal. Then, since swapping the i^{th} and j^{th} row of M gives you the same matrix as swapping the i^{th} and j^{th} column of M, then the i^{th} entry along the diagonal must equal the j^{th} entry along the diagonal, for all i and j. Therefore, M must be a multiple of I_n. Finally, it is easy to see that all nonzero multiples of I_n do commute with all $N \in G$. So the proposition is proved for $Z(GL_n(F))$. The proof for $Z(SL_n(F))$ is similar.