Some matrix groups

Minhyong Kim

October 1, 2005

We've discussed the situation of

$$G \leq \mathrm{Aut}(X)$$

where X is some set. One usually considers the full group $\mathrm{Aut}(X)$ only when X is a finite set, and otherwise studies examples of G that are defined by the condition of preserving some extra structure. Some cases of this are more important than others. For example, when X is a vector space we may take G to be the automorphisms that preserve the linear structure. If $X = k^n$ for a field k, then $G = GL_n(k)$. One gets further subgroups $H \leq GL_n(k)$ by requiring more structure to be preserved. For concreteness, let $k = \mathbb{R}$. Then we have,

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | \det(A) = 1\}$$

$$O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | A^T A = Id\}$$

Recall that the first group can be thought of as the linear transformations that preserve *volume* and *orientation*, while the second consists of linear maps that preserve distance. (On the other hand, we showed in class that if a map simply preserves the *origin* and distance, then it is automatically linear.) We can combine the two conditions to get

$$SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$$

One gets a whole class of examples by fixing matrices $Q \in M_n(\mathbb{R})$, and defining

$$G_Q = \{A \in GL_n(\mathbb{R}) | A^T Q A = Q\}$$

Question: What is G_Q when $Q = Id$? When $Q = \mathrm{diag}(1, -1, -1, -1)$?
Each Q defines a *bilinear form* on $\mathbb{R}^n \times \mathbb{R}^n$,

$$f_Q(x, y) := x^T Q y$$

and G_Q consists exact of those invertible A such that

$$f_Q(Ax, Ay) = f_Q(x, y)$$

for all $x, y \in \mathbb{R}^n$. In the important special cases where Q is symmetric, i.e., $Q^T = Q$, then there are not that many 'essentially different' examples. To explain this, define $Q \sim Q'$ if $Q' = g^T Q g$ for some $g \in GL_n(\mathbb{R})$ and say Q is equivalent to Q'.

Exercise: If $Q \sim Q'$, then $G_Q \simeq G_{Q'}$.

We can understand this in terms of group actions. The action in question is that of $GL_n(\mathbb{R})$ on $M_n(\mathbb{R})$ by $g \cdot L = g^T L g$. Then G_Q is just the stabilizer subgroup of Q. $Q \sim Q'$ is just saying that they are in the same orbit of this action. Thus, the stablizers are isomorphic (in fact, conjugate in $GL_n(\mathbb{R})$).

There is a a theorem of Sylvester that says any symmetric Q is equivalent to

$$\mathrm{diag}(1, 1, \ldots, 1, -1, -1, \ldots, -1, 0, 0, \ldots, 0)$$

The total number of zeroes is called the *nullity* of Q, while $n-$ (nullity) is called the rank. The difference between the number of positive signs and negative signs is called the *signature* of Q. Note that the theorems says that the orbit of Q, and hence G_Q is completely determined by the rank r and signature s. (There are reasons for encoding the info in r and s, rather than, say, r and the number of positive signs. But an explanation of this would be rather elaborate.) Thus, for a given n, we get only finitely many groups this way. Consider for yourself the difference from the case of action by conjugation.

If $r = n$, we say Q is non-degenerate (this case is more important than the degenerate). In that case,

$$Q \sim \mathrm{diag}(1, 1, \ldots, 1, -1, -1, \ldots, -1)$$

and G_Q for this diagonal matrix is sometimes written $O_{k,n-k}(\mathbb{R})$, where k is the number of 1's. As you know, $O_{1,3}(\mathbb{R})$ is called the Lorentz group, and is very important in the special theory of relativity. Elements of the Lorentz group relate the viewpoints (that is, orthogonal coordinatization of space and measure of time) of two observers moving uniformly with respect to each other.

Another important case is when $n = 2m$ and we take Q to be the matrix

$$J = \begin{pmatrix} 0 & -Id_m \\ Id_m & 0 \end{pmatrix}$$

Then G_Q is denoted $Sp_{2m}(\mathbb{R})$ and called the *symplectic group.* It is important in classical mechanics, among other things. (Read just the first chapter of the nice book by Guillemin and Sternberg, 'symplectic techniques in physics,' for some pretty examples from optics.)

It is perfectly reasonable to consider the conjugation action and consider subgroups defined by conditions like

$$AQA^{-1} = Q.$$

Of course, we are in the context of the commutator subgroup of a fixed element (If J itself is in $GL_n(\mathbb{C})$.)

One important case is when Q is the J above.

Exercise: Prove that the group $\{A | AJA^{-1} = J\}$ is isomorphic to $GL_m(\mathbb{C})$.

When we consider complex coefficients, there is the action by complex conjugation (don't confuse this sort of conjugation with conjugation by a group element) to use, so we get groups like the unitary group:

$$U_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) | \bar{A}^T A = Id\}$$

Exercise: Inside $GL_{2m}(\mathbb{R})$, consider the subgroups $GL_m(\mathbb{C})$, $O_{2m}(\mathbb{R})$, and $Sp_{2m}(\mathbb{R})$. The intersection of any two of them is $U_n(\mathbb{C})$. (Here, normalize the isomorphism $\mathbb{C}^m \simeq \mathbb{R}^{2m}$ carefully, since this will influence the embedding of $GL_m(\mathbb{C})$.)

For any of these constructions, we can consider 'special linear' versions by imposing the determinant one condition to get, say, SO_n and SU_n. One can also take the quotient by whatever scalar matrices lie inside the group to get 'projective' versions, like

$$PGL_n(\mathbb{R}), PSL_n(\mathbb{R}), PSU_n(\mathbb{C}), \ldots$$

Exercise: $PGL_n(\mathbb{C}) \simeq PSL_n(\mathbb{C})$. Is $PGL_n(\mathbb{R})$ isomorphic to $PSL_n(\mathbb{R})$? Note that PSL_n is in any case always a subgroup of PGL_n.

These constructions can be carried out over arbitrary fields (even rings, with appropriate modifications). Of course, the geometric interpretation in terms of things like distance may not be too clear, but we have interpreted various conditions purely algebraically. Performing such operations over finite fields $\mathbf{F}_q$ gives us finite groups like $PSL_n(\mathbf{F}_q)$.

Question: When is $PSL_n(\mathbf{F}_q)$ isomorphic to $PGL_n(\mathbf{F}_q)$? Is SL_n ever isomorphic to GL_n?

The analogue of the unitary group is slightly more complicated. For this, one considers $\mathbf{F}_{q^2}$ which is a degree two extensions of $\mathbf{F}_q$. That is, $\mathbf{F}_{q^2}$ can be thought of as pairs of elements of $\mathbf{F}_q$ and relates to $\mathbf{F}_q$ like $\mathbb{C}$ relates to $\mathbb{R}$. Thus, there is an automorphism σ of $\mathbf{F}_{q^2}$ whose fixed field is $\mathbf{F}_q$. This is like complex conjugation. Then we can define

$$U_n(\mathbf{F}_{q^2}) = \{A \in GL_n(\mathbf{F}_{q^2}) | \sigma(A^T)A = Id\}$$

(Here, σ is just acting on the entries of a matrix.)

Many series of finite simple groups can be obtained via such matrix constructions (and more complicated ones). For example, $PSL_n(\mathbf{F}_q)$ is simple for all $n \geq 2$ except when $n = 2$ and $q = 2, 3$. (What happens in these cases?) $PSU_n(\mathbf{F}_{q^2})$ is simple for $n \geq 2$ unless $(n, q^2) = (2, 4), (2, 9), (3, 4)$. $PSp_{2m}(\mathbf{F}_q)$ is simple for $2m \geq 2$ unless $(2m, q) = (2, 2), (2, 3), (4, 2)$. (In all cases, the point is that the smallest few cases are ruled out by a process similar to what you did in the exercises.) Such simple groups are said to be of *Lie type.* (By the way, you should ask yourself why we need all these S's and P's. Why not just consider GL's?)

We have thus far met three infinite series of finite simple groups

(1) $\mathbb{Z}/p$ for p a prime;

(2) A_n, for $n \geq 5$.

(3) Finite simple groups of Lie type. (Well, we haven't really met them, but we've seen the easiest examples.)

The classification theorem says that there are only 26 more finite simple groups, the so-called *sporadic* simple groups. The largest of them, the subject of much mystery, wild speculation, and deep research, is called the *monster group* and is denoted F_1. (Don't confuse with the notation for finite fields.) It has order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

and admits a very famous homomorphism

$$F_1 \rightarrow GL_{196883}(\mathbb{C})$$

first constructed using ideas of string theory. In this context, you should make yourself aware as soon as possible that homomorphisms to matrix groups are very important, even when studying groups given in some other fashion. Such homomorphisms are called *(linear) representations* of the group. One says, for example, that the monster group has a 196883-dimensional representation.

It is interesting that matrix groups can show up in situations where the structure preserved is not a priori linear. For example, let $\mathbb{H} := \{x + iy | y > 0\} \subset \mathbb{C}$ be the upper-half plane. Since we know what an analytic function is, we can consider $An(\mathbb{H})$, the group of *analytic automorphisms* of $\mathbb{H}$. Earlier on, we had constructed a homomorphism

$$PSL_2(\mathbb{R}) \rightarrow An(\mathbb{H})$$

which was actually an injection. Rather surprisingly, this map is an isomorphism. $\mathbb{H}$ of course does not have any obvious natural linear structure, and the transformations are not linear ones in the usual sense (they are often called 'fractional linear' transformations). Also, to get rid of any remnant of linearity, use the Riemann mapping theorem to replace $\mathbb{H}$ by any strangely-shaped simply-connected domain U in $\mathbb{C}$. Then

$$PSL_2(\mathbb{R}) \simeq An(U)$$

For a much simpler example, recall that the automorphism group of the three-element set is isomorphic to $SL_2(\mathbf{F}_3)$.