34 Simple Linear Groups

34.1 Review

Last time, we took a group $G \leq GL_n(\mathbb{R})$ and looked at $\text{Lie}(G)$, the vector space of tangent vectors at the identity. We had lots of different definitions, but the most familiar way is to think of $\text{Lie}(G)$ as all the matrices that provide one-parameter groups inside of G. The key point was that not only is $\text{Lie}(G)$ a vector space, but it also has some extra structure: the Lie bracket $[A, B] = AB - BA$, which is a skew-symmetric multiplication on the vector space. This is a new operation, but it also arises naturally from considering multiplication on G, and sort of taking its derivative. The Lie bracket measures the failure of G to be commutative.

We don't actually need G to be a subgroup of $GL_n(\mathbb{R})$ in order to do this. For any group with a manifold structure, called a **Lie group**, we can look at the tangent vectors through the identity, and we get a vector space which also has a bracket multiplication, which is its **Lie algebra** $\text{Lie}(G)$.

Student Question. *Can you recover the group from its Lie algebra?*

Answer. *In general, the answer is no. For example, SU_2 and SO_3 have the same Lie algebra. But it turns out that if two groups have the same Lie algebra, they're related to each other – here SU_2 and SO_3 differ by a "finite amount" (we have a two-to-one surjection $SU_2 \to SO_3$), and you can show something similar is true in general. In fact, if you require the group to be simply connected, then there is a unique group with a given Lie algebra. You can then use this to study all the groups with a given Lie algebra.*

This ends up being a powerful tool because now in order to understand a group with a manifold structure, we can instead try to understand its Lie algebra, which is an easier problem; and then figure out how to go backwards.

34.2 Simple Linear Groups

Recall that a group is **simple** if its only normal subgroups are the trivial group and the whole group. You can think of simple groups as building blocks for more complicated groups – if you have a group that isn't simple, then you can understand it by understanding the normal subgroup and its quotient group. But if you have a simple group, you can't break it down further.

> **Guiding Question**
> Which $G \leq GL_n(\mathbb{R})$ are simple?

We'll look at two groups: SU_2 and SL_2.

34.3 The Special Unitary Group

First we'll look at whether SU_2 is simple. The answer is no – the center of a group (the set of elements which commute with everything) is always a normal subgroup. But the center of SU_2 is $\pm I$, which is nontrivial.

But it turns out that's essentially the only thing that can happen:

> **Theorem 34.1**
> If $N \trianglelefteq SU_2$, then N must be $\{I\}$, SU_2, or $\{\pm I\}$.

So then in order to produce a simple group, we can quotient out by this center:

> **Corollary 34.2**
> The quotient $SU_2/\{\pm I\}$ is simple.

This quotient is actually SO_3: we have a surjective homomorphism $SU_2 \to SO_3$ (from the conjugation action on the equator), and the kernel is exactly $\{\pm I\}$. So in particular, SO_3 is simple.

Proof of Corollary 34.2. This follows from the Correspondence Principle: we have a surjection $\varphi : SU_2 \to SO_3$. So for any normal subgroup $N \trianglelefteq SO_3$, its pre-image is a subgroup of SU_2, which is also normal and contains the kernel $\{\pm I\}$. But any normal subgroup of SU_2 containing the kernel is equal to either the kernel or the

whole group, which means the initial normal subgroup in SO_3 is either the identity or the entire group (by taking the image under φ). □

Proof of Theorem 34.1. We can use the geometric intuition of what SU_2 looks like. It's a 3-sphere in 4-dimensional space, and its conjugacy classes are exactly the latitudes – the 2-spheres we get from taking horizontal slices.

Suppose we have $N \trianglelefteq SU_2$, and some element $Q \in N$ which is not $\pm I$. We'd like to show that N must then be the entire group.
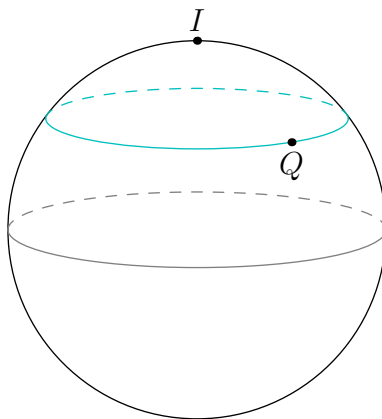

Since N is normal, everything conjugate to Q must also be in N. If $\text{Tr}(Q) = 2c$, then Lat_c is the conjugacy class of Q, so this entire latitude must be inside N. (This latitude is a 2-sphere of positive radius, since Q is not $\pm I$.)

Now we can take this 2-sphere, and translate it to pass through the identity: consider $Q^{-1} \text{Lat}_c$, which is a 2-sphere (of positive radius) passing through the north pole I. This must also be contained inside N (since Q and Lat_c are both contained inside N).
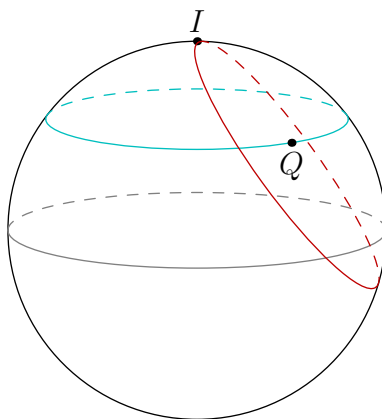

Now start at I, and take a nontrivial path inside this two-sphere. Write this path as $f(t)$ for $0 \le t \le \varepsilon$, where we have $f(t) \in Q^{-1} \text{Lat}_c$ for all t, and $f(0) = I$, while $f(t) \ne I$ for $t > 0$.
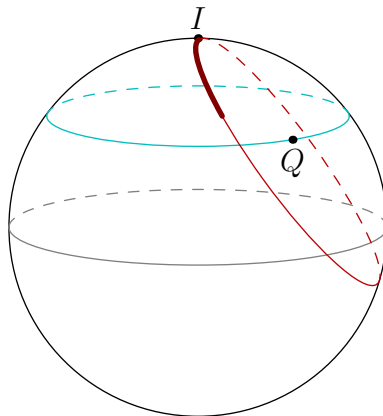
Then $f(t)$ is contained in $Q^{-1}\operatorname{Lat}_c$, and therefore inside N. And the north pole is the only point in the sphere with trace 2, so $\operatorname{Tr}(f(t)) < 2$ for all $t > 0$. This means there exists some $\delta > 0$ such that for all $2 - \delta < c < 2$, there exists t such that $\operatorname{Tr}(f(t)) = c$.

But once we find that N contains one point on a given latitude, then N must contain *every* point on that latitude (because N is normal, so it must contain the entire conjugacy class of that point). So this means for every c such that $2 - \delta < c < 2$, the latitude $\operatorname{Lat}_{c/2}$ is contained inside N.
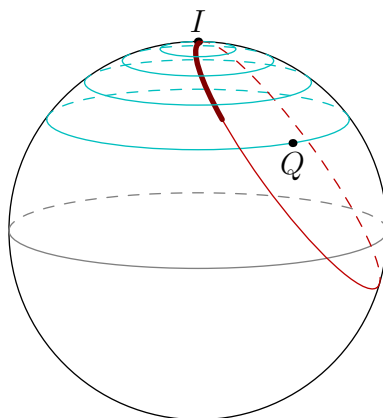
This means we have an entire neighborhood of the identity that's contained inside N – any point $A \in SU_2$ with $\operatorname{Tr}(A) > 2 - \delta$ is contained inside N.

Now we're almost done: we want to show that once we have a neighborhood of the identity, we have all points. To do this, we can look at the longitudes: pick some v on the equator, and look at $\operatorname{Long}_v \leq SU_2$. Every point on the three-sphere is in some longitude, so it suffices to show that every longitude is contained in N.
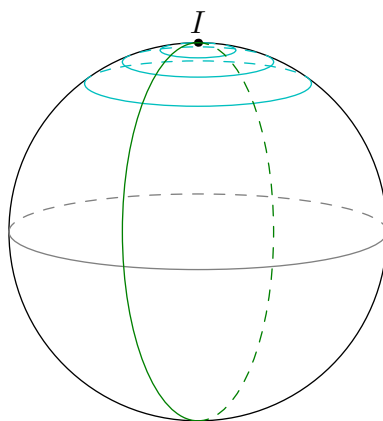
But this longitude is the circle

$$\{\cos\theta I + \sin\theta v \mid 0 \le \theta < 2\pi\}.$$

And we know that if θ is small enough, then the point ρ_θ corresponding to θ is in N (meaning there exists ε such that $\rho_\theta \in N$ for all $|\theta| < \varepsilon$).
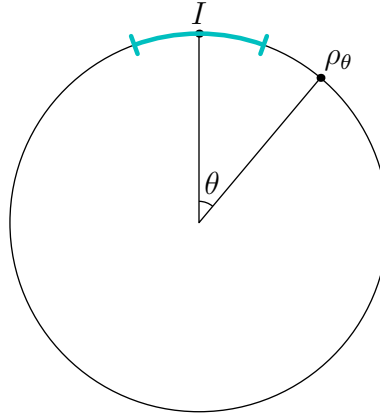
Now we can take ρ_θ for small θ, and multiply it by itself repeatedly to cover the entire circle: for any $\varphi \in [0, 2\pi)$, there is some M such that $\frac{\varphi}{M} < \varepsilon$. Then $\rho_{\phi/M}$ is in N, which means $\rho_\varphi = (\rho_{\varphi/M})^M$ is in N as well.

So now every longitude is in N, and since every point is in a longitude, this means all of SU_2 is in N. $\qquad\square$

> **Note 34.3**
>
> This is a really hands-on argument; we used the fact that we have both a geometric and group-theoretic understanding of what SU_2 is.

34.4 The Special Linear Group

Now we'll look at $SL_2(\mathbb{C})$ – the group of 2×2 matrices with determinant 1.

Again, $\pm I$ is the center of $SL_2(\mathbb{C})$, so the most we could ask for is that if we quotient out by this normal subgroup, we get a simple group. It turns out that this is the case, and it actually works for *any* field F, not just the complex numbers:

> **Theorem 34.4**
>
> For any field F with $|F| \ge 4$, the quotient $SL_2(F)/\{\pm I\}$ is simple.

This quotient is sometimes called $PSL_2(F)$.

We're no longer in a geometric setting (F can be a finite field), so the proof won't be geometric like the previous one; instead, we'll get our hands on generators and relations.

> **Note 34.5**
>
> The theorem is false over $\mathbb{F}_2$ and $\mathbb{F}_3$. This is similar to how when we looked at the alternating groups, we saw that A_n is simple for all $n \ge 5$, but A_4 and A_3 are not simple. In both cases, we have a family of groups where the first couple may be counterexamples, but eventually they all become simple.

Proof of Theorem 34.4. We'll prove this in the case where $|F| > 5$ (there's only two remaining cases, which can be checked by hand). It suffices to prove that if we have a normal subgroup $N \trianglelefteq SL_2(F)$, then N is either $\{I\}$, $\{\pm I\}$, or $SL_2(F)$ – then this implies the quotient is simple by the same argument as before, using the Correspondence Principle.

We'll begin with a few lemmas about the field:

> **Lemma 34.6**
> Given $a \in F$, the equation $x^2 = a$ has at most 2 solutions.

This seems obvious, but it's possible to have more solutions in $\mathbb{Z}/n\mathbb{Z}$ if n is not prime. So it matters that F is a field.

Proof. If we have two solutions x and y, then $x^2 = y^2$, so

$$(x + y)(x - y) = 0.$$

But because F is a field, if two elements multiply to 0, then one of them is 0. So either $x = y$ or $x = -y$; this means if there's one solution, then there's at most one other solution. $\square$

> **Lemma 34.7**
> If $|F| > 5$, then there exists some $r \in F$ such that r^2 is not 0, 1, or -1.

Proof. There's at most one square root of 0, two square roots of 1, and two square roots of -1. So there are at most five bad elements; and as long as there are more than 5 elements in the field, we can find some good element (whose square isn't 0 or ± 1). $\square$

Now we'll prove the main theorem. Fix an element r with $r^2 \notin \{0, 1, -1\}$. Assume that we have a normal subgroup $N \trianglelefteq SL_2(F)$ containing some element other than $\pm I$; then we'll show that N is the entire group.

Claim 34.8. *We can find some $B \in N$ with distinct eigenvalues.*

Proof. Pick some $A \in N$, with $A \neq \pm I$. Then A is not a scalar matrix, so there is some vector $v_1 \in F^2$ which is not an eigenvector of A. Then take $v_2 = Av_1$. Since v_1 is not an eigenvector, v_1 and v_2 are linearly independent, so $\{v_1, v_2\}$ is a basis for F^2.

Now define $P \in GL_2(F)$ with the property that $Pv_1 = rv_1$ and $Pv_2 = r^{-1}v_2$. Then P is diagonal in the basis $\{v_1, v_2\}$, and its eigenvalues are r and r^{-1}. So the determinant of P is 1, which means $P \in SL_2(F)$.

We don't know whether P is in N. But we can define $B = APA^{-1}P^{-1}$. We claim that B is inside N – we know A is in N. Meanwhile, $PA^{-1}P^{-1}$ is the conjugate of an element of N, so it must also be in N (since N is normal). Since N is a subgroup, their product must be in N as well.

But we have
$$Bv_2 = APA^{-1}P^{-1}v_2 = APA^{-1}rv_2 = APrv_1 = Ar^2v_1 = r^2v_2.$$

So r^2 is an eigenvalue of B, and r^{-2} is the other eigenvalue (because $\det B = 1$). By our choice of r, we have $r^2 \neq r^{-2}$, since $r^2 \neq \pm 1$. So this concludes the first step. $\square$

Set $s = r^2$, so we have a matrix $B \in N$ with distinct eigenvalues s and s^{-1}.

Claim 34.9. *All matrices in SL_2 with eigenvalues s and s^{-1} are contained in N.*

Proof. We'll show that this set of matrices is actually a single conjugacy class in SL_2. It contains B, so then since N is normal, this implies the entire set is contained in N.

Given Q with eigenvalues s and s^{-1}, we know Q is diagonalizable (since it has distinct eigenvalues), so we have

$$LQL^{-1} = \begin{bmatrix} s & 0 \\ 0 & s^{-1} \end{bmatrix}$$

for some $L \in GL_2(F)$. Then we can take

$$L' = \begin{bmatrix} \det L^{-1} & 0 \\ 0 & 1 \end{bmatrix} L.$$

This has determinant 1, so it's in SL_2; and it has the same property (that that $L'QL'^{-1}$ is diagonal). So all matrices with eigenvalues s and s^{-1} are in the same conjugacy class of SL_2. $\square$

To finish, we can look at all matrices generated (as a group) by the matrices with eigenvalues s and s^{-1}. We can get a huge collection of matrices like this: for example, we can show that any matrices of the form

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$$

are in this group. Then there was a homework question from a long time ago that showed matrices of these forms generate all of SL_2. $\qquad\square$

Both our proofs had similar ideas: find some element in the normal subgroup, conjugate it to find a whole bunch of elements in the normal subgroup, and use those elements to generate the entire group.

34.5   Generalizations

We focused on 2×2 matrices here, but these examples are actually typical, and generalize to higher dimensions.

If a subgroup $G \leq GL_n(\mathbb{C})$ is defined by polynomial constraints (for example, we can require that the matrix has determinant 1, but we can't take complex conjugates – so the unitary groups are not in this category, but the orthogonal groups are), then you can actually classify which ones are simple. We've essentially seen these already: you can take SL_n modulo its center, and SO_n modulo its center. You can also take a *skew-symmetric* form instead (which we didn't really discuss in class), modulo its center. These are almost all the simple groups – there's just five other examples.

The proof uses the idea of passing to the Lie algebra $\text{Lie}(G)$ – you first understand what a simple Lie algebra is, and use that to study what the simple Lie groups are.

The really remarkable thing is that understanding these matrix groups also lets you understand finite simple groups – if you replace $\mathbb{C}$ with a finite field, then these examples give *finite* simple groups, and these are almost all the known examples (with 26 exceptions).