Lecture 9-30: Finite subgroups of $SO_3(\mathbb{R})$ and the Sylow theorems

September 30, 2024

I have exhibited three important and interesting finite symmetry groups lying in $G = SO_3(\mathbb{R})$, namely the alternating groups A_4 and A_5 and the symmetric group S_4. Today I will show that these groups account for all the finite subgroups of G, apart from the cyclic and dihedral groups. I will also state the Sylow theorems, which you will prove in homework, using the left translation action of a finite group on itself.

I will warm up by looking at the groups $O_2(\mathbb{R})$ and $SO_2(\mathbb{R})$ of orthogonal and special orthogonal 2×2 matrices. It is well known and easy to check that an orthogonal 2×2 matrix with determinant one takes the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for some $\theta \in \mathbb{R}$; this is the matrix M_θ of counterclockwise rotation by θ radians.

An orthogonal 2×2 matrix of determinant -1 takes the form $\begin{pmatrix} -\cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for some θ; this is the matrix of a reflection. A finite subgroup F of $SO_2(\mathbb{R})$ will contain M_θ for a unique smallest positive θ, whence it is easy to see that this minimal $\theta = 2\pi/n$ for some positive integer n and F is the cyclic group C_n of order n generated by M_θ. A finite subgroup F of $O_2(\mathbb{R})$ not lying in $SO_2(\mathbb{R})$ is then generated by C_n and a single reflection; it is the dihedral group D_n of symmetries of a regular n-gon in the plane.

Any matrix $M \in O_2(\mathbb{R})$ can be enlarged to a matrix in $G = SO_3(\mathbb{R})$ by adding a third row and column, each consisting of two 0s and a 1 if $M \in SO_2(\mathbb{R})$ and two 0s and a -1 if $M \notin SO_2(\mathbb{R})$. Thus the cyclic and dihedral groups C_n, D_n are indeed finite subgroups of G. To analyze the other finite subgroups of G, begin by observing for any $M \in G$ the difference $M - I$ (I the identity matrix) is such that its determinant equals that of $(M - I)M^t$ by the product rule for determinants, which in turn equals $\det(I - M^t) = \det(I - M)^t = \det(I - M) = -\det(M - I)$, since $I - M$ is obtained from $M - I$ by changing the signs of all entires in its three columns. It follows that $\det(M - I) = 0$, so that M always has 1 as an eigenvalue. Let $v \neq 0$ be a corresponding eigenvector, we see that M preserves the plane orthogonal to v in $\mathbb{R}^3$, whence it must act on this plane by a rotation (not a reflection, since it has determinant 1). Thus every nonidenity orientation-preserving orthogonal transformation M in $\mathbb{R}^3$ is a rotation about a unique axis.

In particular such an M necessarily fixes a unique pair $\pm v$ of unit vectors in $\mathbb{R}^3$. Call these its poles. Given now a finite subgroup F of G, let P be the set of poles of its nonidentity elements. If p is a pole of some $f \in F$ and $g \in F$, then gp is a pole of the conjugate gfg^{-1} of f in F, whence F acts on the finite set P. Now I count the poles in P in two ways, counting each k times if it is the pole of k distinct nonidentity elements of F. Let N be the order of F. On the one hand, every one of the $N-1$ nonidentity elements of F has exactly two poles, so there are $2(N-1)$ poles altogether. On the other, every pole p is a pole of $n-1$ nonidentity elements of F, where n is the order of the stabilizer of p in F. There are $\frac{N}{n}$ poles in the orbit of p, each having stabilizer of order n, by the Orbit Formula, so if there are say k orbits of F in P and n_i be the order of the stabilizer of any element of the ith orbit, then we get

$$2(N-1) = \sum_{i=1}^{k} \frac{N}{n_i}(n_i - 1).$$

Dividing by N we deduce that

$$2 - \frac{2}{N} = \sum_{i=1}^{k} (1 - \frac{1}{n_i})$$

Now each n_i is at least 2, so that every term on the right side is at least $\frac{1}{2}$, while the left side is less than 2. Hence there can be at most 3 orbits. But there cannot be one orbit, lest the left side be at least 1 while the right side is less than 1, so there are exactly two or three orbits.

If there are two orbits we get

$$2 - \frac{2}{N} = (1 - \frac{1}{n_1}) + (1 - \frac{1}{n_2});$$

recalling that each n_i divides N, we see that this forces $n_1 = n_2 = N$. In this case there are just two distinct poles p_1, p_2, every nonidentity element of F has the p_i as its poles, and each pole p_i forms an orbit by itself. In this case $F \cong C_n$ is the group of rotational symmetries of a regular n-gon in the plane. The poles are a point above this plane containing the n-gon and its reflection through this plane to the point symmetrically below it.

If there are three orbits we get $2-\frac{2}{N}=(1-\frac{1}{n_1})+(1-\frac{1}{n_2})+(1-\frac{1}{n_3})$, forcing $\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{n_3}>1$. Relabelling so that $n_1 \leq n_2 \leq n_3$ and recalling that each n_i is at least 2, we find that that there is one family of solutions to the displayed equation, namely $n_1=n_2=2, n_3=\frac{N}{2}$, and three isolated solutions, namely $n_1=2, n_2=n_3=3, N=12; n_1=2, n_2=3, n_3=4, N=24$; and finally $n_1=2, n_2=3, n_3=5, N=60$.

In the first case, the three orbits of poles turn out to be the vertices and the midpoints of the sides of a regular ($n = \frac{N}{2}$)-gon in the plane (rescaled so as to have length 1), together with the two points above and below this plane mentioned in the two-orbit case. This time these two points come together in a single orbit and the group F is the full symmetry group D_n of the regular n-gon.

In the other three cases the three orbits of poles are the vertices, midpoints of the edges, and centers of the faces of a regular polyhedron in $\mathbb{R}^3$ (again rescaled to have length 1) and F is the orientation-preserving symmetry group of this polyhedron. For example, in the last case, the first orbit consists of the midpoints of the 30 edges of either a dodecahedron or an icosahedron, while the other two orbits consist of the twenty vertices (say of the dodecahedron) and the twelve centers of its faces. The stabilizer of the center of a face coincides with the stabilizer of the face, which consists of five rotational symmetries of a pentagon. The stabilizer of a vertex consists of the three rotational symmetries of the equilateral triangle formed by the three other vertices closest to the given one. A similar analysis applies in the other cases. The only other possibilities for F (besides C_n and D_n) are thus A_4, S_4, and A_5, as claimed.

This last argument is not in Dummit and Foote, but can be found for example in Michael's Artin's text "Algebra", whose second edition was published in 2010.

Turning again to to a more abstract setting, let G be a finite group and p a prime. Write the order $|G|$ of G as $p^k m$, where $\not| m$.

Sylow's Theorem: Theorem 18, p. 139

- G has a subgroup of order p^k (a *p-Sylow subgroup*)
- Any two p-Sylow subgroups are conjugate in G.
- The number n_p of p-Sylow subgroups is congruent to $1 \bmod p$ and divides the index m of any such subgroup

You will prove this in homework this week; along the way you will also prove that the number $n_{p,\ell}$ of subgroups of G of order p^ℓ is congruent to 1 mod p for any $\ell \leq k$.

Sylow's Theorem has many consequences for the structure of finite groups (though it does not by any means classify all such groups up to isomorphism). For example, let p, q be distinct primes with $p > q$ and let G be a group of order pq. The number n_p of p-Sylow subgroups of G divides q and is congruent to 1 mod p, whence it must be 1, so that the unique p-Sylow subgroup is normal. The same holds for the number n_q of q-Sylow subgroups provided that p is not congruent to 1 mod q. In this case then G has normal cyclic subgroups G_p, G_q of orders p and q, whence by counting elements one sees that $G = G_p G_q, G_p \cap G_q = 1$. Then G is isomorphic to the direct product $\mathbb{Z}_p \times \mathbb{Z}_q$ of cyclic groups of orders p and q, whence by a standard elementary result G is itself cyclic of order pq: if p and q are distinct primes with neither one congruent to 1 modulo the other, then any group of order pq is cyclic. See p. 143.

What if the larger prime p is congruent to 1 modulo the smaller one q? In this case the number of q-Sylow subgroups need not be 1, so that a q-Sylow subgroup of a group G of order pq need not be normal. We still have all the ingredients necessary, however, to realize G as the *semidirect* product of cyclic subgroups G_p, G_q of orders p and q, with the former group acting on the latter one by automorphisms. More precisely, the automorphism group Aut G_q turns out to be cyclic of order $q - 1$ (as I will show later), so that it admits a unique cyclic subgroup of order p. Consequently, if p, q are distinct primes with p congruent to 1 mod q, then there is a unique nonabelian group of order pq up to isomorphism, which is a semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_p$.