Math 504, 9/28

I will begin with group theory, starting with group actions on sets. Given a group G and a set S, an action of G on S is a rule that assigns to each pair (g, s) in GxS an element t of S, usually denoted gs, such that $1s = s$ for all s in S, where i is the identity element of G and $h(gs) = (hg)s$ for g, h in G, s in S. (More precisely, this defines a **left** action of G on S; had we written sg for the action of the element g on the element s, the natural axiom would have been $(sg)h = s(gh)$; this defines a **right** action). It is not difficult to verify that a left action of G on S is equivalent to a homomorphism π from G to the permutation group $\mathrm{Perm}(S)$ of all bijections from S to S, where we decree that $\pi(g)(s) = gs$, where gs is the action of g on s. If G acts on S and s is an element of S, then the set of g in G such that $gs = s$ is an important subgroup of G, called the **stabilizer** of s and denoted G^s. Likewise, we have an important subset Gs of S, defined to be the set of all gs as g runs through G and called the orbit of s. If $H = G^s$, then it is easy to check that any two elements of the same left coset gH of H in G map s to the same element, and in fact two elements of G map s to the same element if and only if they lie in the same left coset of H in G. If G is finite, it follows by Lagrange's Theorem (which I assume you have seen) that the order $|G|$ of G equals the product of the orders $|G^s||Gs|$ of the orders of the orbit and stabilizer of any s in S: this important formula, called the Orbit Formula, will be used constantly in this course (and beyond). If the set S has only one G-orbit, then we call the G-action on it *transitive*; in this case we can of course replace the orbit Gs in the Orbit Formula by the entire set S. In general, no two orbits of G in S can overlap, so another useful formula, if S is finite, is that its order equals the sum of the orders of the orbits in it.

An important but all too rarely seen example occurs when G is a finite subgroup of SO_3; that is, a finite group of 3 x 3 real matrices M of determinant 1 such that the transpose M^t of M equals its inverse M^{-1}, or equivalently such that M preserves dot products in R^3: $Mv \cdot Mw = v \cdot w$ for all vectors v, w in R^3. Any such matrix M is such that $\det(M - I) = \det(M^t - I^t) = \det(M^{-1} - I) = \det(M^{-1} - I)(\det M) = \det(I - M) = -\det(M - I) = 0$, whence M has an eigenvalue 1 and must fix some nonzero vector v in R^3. But then M preserves the plane in R^3 perpendicular to v, whence it acts by a rotation in this plane. It follows that M is either the identity or fixes exactly two unit vectors in R^3 (each the negative of the other), acting by a rotation about the line through these vectors, which also goes through the origin. Thus any g in G with $g \neq 1$ has exactly two poles. If N is the order of G, there are $2(N - 1)$ poles in R^3 of nonidentity elements of G, counting each as often as it appears as the pole of a nonidentity element. On the other hand, if p is a pole of some element of g and h is any other element of G, then hp is a pole of hgh^{-1}, so G acts on the set P of poles of its nonidentity elements. Each pole p_i in P will have a stabilizer G^p consisting of finitely many rotations in G; if there are r_i such rotations, then the number n_i of elements in the orbit of p satisfies $r_i n_i = N$. Counting the number of poles again, this time for each pole counting the number of nonidentity elements of G fixing it and observing that this number is the same for any pole in the orbit of p, we get $\sum n_i(r_i - 1)$, where there is one index i for every orbit of poles in G. Hence

$$2(N-1) = \sum_i n_i(r_i - 1)$$

where the number of terms in the sum equals the number of orbits. Dividing both sides by N, we get

$$2(1 - 1/N) = \sum_i (1 - (1/r_i))$$

using again that $n_i r_i = N$, by the Orbit Formula. But now the left side is less than 2, while every term in the right side is at least $1/2$, so there are at most 3 orbits. More precisely, the left side is at least 1 and each term on the right side is less than 1, so there cannot be just one orbit. If there are two orbits, then we must have $r_1 = r_2 = N$ (since r_1 and r_2 are less than N). In this case there are exactly two poles, each lying in an orbit by itself. The group G must be a cyclic group, consisting of rotations by multiples of $2\pi/N$ about a fixed axis. If there are three orbits, then $(1/r_1) + (1/r_2) + ()1/r_3) > 1$. We will work out the consequences of this elementary but very famous inequality and (sketch) a classification of the groups G arising in this way next time. A reference for this material is Artin's book *Algebra*, on reserve (and in the stacks) of the Math Library.