Math 122, PSET 8 Answer Key (With special, special thanks to Sam Lichtenstein, from whom I have directly taken with permission the code and solutions for all of the following questions except for number 8.)
Daniel Gardiner

(1) **Claim.** If $p, q \in S_n$ then pq and qp have cycles of equal sizes.
Proof. Since $q(pq)q^{-1} = qp$, we know that pq and qp are conjugate to one another. Then by Artin's Prop. 6.6.10.(c) we know that their cycle decompositions have the same orders. □

(2) If $\sigma = (i_1^1 \dots i_{k_1}^1)(i_1^2 \dots i_{k_2}^2) \dots (i_1^m \dots i_{k_m}^m)$ is a permutation in S_n written as a product of cycles, we can determine its sign in the following manner. Since an elementary calculation verifies that $(i_1^j \dots i_{k_j}^j) = (i_1^j\, i_{k_j}^j)(i_1^j\, i_{k_j-1}^j)(i_1^j\, i_{k_j-2}^j) \dots (i_1^j\, i_3^j)(i_1^j\, i_2^j)$ is a product of $k_j - 1$ transpositions, we have that $\operatorname{sgn}(i_1^j \dots i_{k_j}^j) = (-1)^{k_j - 1}$. Hence $\operatorname{sgn}\sigma = \prod_j (-1)^{k_j - 1} = (-1)^{(\sum_j k_j) - m}$. That is, to find the sign of σ we add the orders of all the cycles, subtract the number of cycles, and look at whether the result is even or odd. If it is odd, so is σ; if it is even, so is σ.

(3) (a) **Claim.** Let the disjoint cycle decomposition of $\sigma \in S_n$ be $\sigma = (i_1^1 \dots i_{k_1}^1)(i_1^2 \dots i_{k_2}^2) \dots (i_1^m \dots i_{k_m}^m)$. Then the order of σ is the least common multiple of the k_j.
Proof. Let $N = \operatorname{lcm}\{k_j\}$. Since disjoint cycles have disjoint support, a result from lecture (or cf. problem (7) below) shows that the cycles commute with one another. Hence

$$\sigma^a = [(i_1^1 \dots i_{k_1}^1)(i_1^2 \dots i_{k_2}^2) \dots (i_1^m \dots i_{k_m}^m)]^a = (i_1^1 \dots i_{k_1}^1)^a (i_1^2 \dots i_{k_2}^2)^a \dots (i_1^m \dots i_{k_m}^m)^a.$$

But each $(i_1^j \dots i_{k_j}^j)^{k_j} = e$ and $k_j | N$ for all j, so $\sigma^N = e$. Therefore the order of σ divides N. But also, because the cycles are disjoint, $\sigma^a = e$ if and only if the ath power of each cycle is the identity (since powers of disjoint cycles cannot be inverses of one another). Therefore the order of each cycle k_j must divide the order of σ. But this implies that $N = \operatorname{lcm}\{k_j\}$ divides the order of σ, so $|\sigma| = N$. □

(b) **Claim.** S_7 contains elements of orders 5 and 10, but not of order 15.
Proof. We exhibit (12345) and (12)(34567) as elements of orders 5 and 10 respectively. But suppose $\sigma \in S_7$ had order 15. Then if σ were written as a product of disjoint cycles, the least common multiple of their lengths would be 15. Hence one cycle would have to be of length at least 5, and another cycle disjoint to the first would have to be of length at least 3. But this would require the use of 8 letters, and $\sigma \in S_7$ is a permutation of only 7 letters. Contradiction. □

(c) **Claim.** The largest possible order of an element in S_7 is 12.
Proof. We wish to maximize $\operatorname{lcm}\{k_j\}$ subject to the constraint $\sum k_j = 7$. Writing all possible partitions of seven letters into disjoint cycles, we find that the maximum order is obtained with permutations of the form $(abc)(defg)$, which have order 12. □

(4) The subgroups of S_4 of order 4 are

$$\langle(1234)\rangle, \quad \langle(1324)\rangle, \quad \langle(1243)\rangle \qquad (\simeq \mathbb{Z}/4\mathbb{Z});$$

$$\{e, (12), (34), (12)(34)\}, \quad \{e, (13), (24), (13)(24)\}, \quad \{e, (14), (23), (14)(23)\}, \quad \{e, (12)(34), (13)(24), (14)(23)\} \qquad (\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}).$$

The only normal subgroup of order 4 is $\{e, (12)(34), (13)(24), (14)(23)\} \lhd S_4$, because all of its elements have cycle decompositions of the same type, and because it contains *every* permutation with that cycle decomposition type.

(5) **Claim.** S_n contains $n!\sum_{k=0}^{n}(-1)^k\frac{1}{k!}$ permutations which do not leave any index fixed.
Proof. Let T be the set of permutations which do not fix any index. To count T, we count its complement $S_n - T$. Denote the collection of permutations fixing the index i by F_i. Then by the principle of inclusion and exclusion,

$$|S_n - T| = \left|\bigcup_{i=1}^{n} F_i\right| = \sum_{k=1}^{n}\sum_{1\le i_1\le\ldots\le i_k\le n}(-1)^{k-1}\left|\bigcap_{j=1}^{k} F_{i_j}\right|.$$

But each term of the inner sum represents $(-1)^{k-1}$ times the number of permutations fixing a given selection of k indices. For any $1 \le k \le n$ there are $\binom{n}{k}$ ways to select k indices to be fixed, and given such a selection there are $(n-k)!$ permutations which fix those k indices. Thus $|\bigcap_{j=1}^{k} F_{i_j}| = (n-1)!$ for each k and there are $\binom{n}{k}$ terms in the inner sum. Hence

$$|S_n - T| = \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)! = \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!}.$$

Subtracting this sum from $|S_n| = n!$ yields the desired result. □

REMARK: Since $\sum_{k=0}^{n}(-1)^k n!/k!$ is an nth order power series for $n!/e$, the number of "derangements" (as permutations fixing no index are called) is actually the same as $[n!/e]$, where the bracket denotes the operation of rounding to the nearest integer. This is very pretty, and easily evaluated for purposes of actual calculation. □

(6) **Claim.** No sequence of moves on a Rubik's Cube switches two edge pieces while leaving the rest unchanged.
Proof. Call the 6 basic moves on the cube f, b, r, l, u, d (for front, back, right, left, up, and down), where the move is counterclockwise rotation of the indicated face by 90 degress. Note that in $G = \langle f, b, r, l, u, d\rangle \subset 1 \times S_8 \times S_{12}$ (permutations of the 8 corners and 12 edges of the cube, leaving the centers of the 6 faces fixed) the permutation specified in the claim is (e, e, τ) for τ a transposition of two edges. This is an odd permutation in $S_{20} \supset G$. However, each generator of the Rubik's cube move group is a permutation of the form $(e, (1234), (1'2'3'4'))$ - that is, each generator cyclically permutes four corners and four edges. In S_{20}, this is a product of two disjoint 4-cycles; by problem (2) above it follows that each generator of G is an even permutation in S_{20}. Hence $G \subset A_{20}$, which means that (e, e, τ) is not in G, since it is odd. Thus, no sequence of moves on the Rubik's cube can produce the desired transposition of two edges. □

(7) **Claim.** If $g, h \in S_n$ have disjoint support then the commutator $[g, h]$ is trivial.
Proof. The commutator $[g, h] = e$ whenever g and h commute. If g and h have disjoint support, then we will show that they commute, proving the claim. (This was proved in lecture, but I shall reproduce the result here.) We must check that $gh(i) = hg(i)$ for any index i. First suppose that i is fixed by *both* g and h. In this case it is clear that $gh(i) = g(i) = i = h(i) = hg(i)$. But if i is not fixed by g then it *must* be fixed by h (and vice versa), because the permutations have disjoint support. So without loss of generality, we can next suppose that i is fixed by g and not h. In this case $hg(i) = h(i)$. Now since $h(i) \neq i$ we know that $h(i) \in \mathrm{Supp}(h)$, so $h(i) \notin \mathrm{Supp}(g)$. Therefore $h(i)$ is fixed by g, so $gh(i) = h(i) = hg(i)$ as desired. Hence g and h commute, so they have a trivial commutator. □

REMARK: The converse is *not* true, for any permutation g and its inverse necessarily have the same support, but also commute with one another, so have trivial commutator $[g, g^{-1}] = e$.

(8) **Claim.** Let $H \subset G$ be the smallest subgroup containing all commutators $[g, g']$ of elements of G.Then $H \lhd G$ and G/H is abelian.

Proof. Take some $h \in H$, $g \in G$. Then the commutator of g and h, $ghg^{-1}h^{-1}$ is in H, so $(ghg^{-1}h^{-1}) * h = ghg^{-1} \in H$. Hence, H is normal in G.

To show that G/H is abelian, observe that $(aH) * (bH) = (ab)H = (ab)(b^{-1}a^{-1}ba)H = (ba)H$ for any $a, b \in G$, where we have used the fact that $b^{-1}a^{-1}ba \in H$ since it is just the commutator of b^{-1} and a^{-1}. Hence G/H is abelian.

Remark: I was generous grading this question, but just a note that technically we only know that H is generated by the commutators. A number of proofs took an arbitrary $h \in H$ and assumed that it was of the form $aba^{-1}b^{-1}$ for some $a, b \in G$, which is not necessarily the case. I didn't take off any points for any of this, but just be more careful in the future.