Gandhar Kulkarni (mmat2304)

1

To prove the result, we will decompose an arbitrary permutation $\sigma \in S_n$ into transpositions. We will then show that each transposition can be written as a product of transpositions of the form $(ii+1)$. We have $\sigma = \tau_1 \dots \tau_r$, where τ_i is some transposition of the form $(k_1k + 1 + k_2)_i$. Note that we can assume the first element of τ_i is strictly lesser than the second since if it weren't we could just invert the order without any loss of generality. We state that $(k_1k_1 + k_2)$ can written as a product of finite transpositions of the form $(tt+1)$. See that $(k_1k_1 + k_2 - 1) = (k_1 + k_2 - 1k_1 + k_2)(k_1k_1 + k_2)(k_1 + k_2 - 1k_1 + k_2)$. Since we have $(k_1k_1 + k_2 - 1)$, we have lowered the second entry of the transposition by one. In $k_2 - 1$ steps, we will get $(k_1k_1 + 1) = (k_1 + 1k_1 + 2)(k_1k_1 + 2)(k_1 + 1k_1 + 2)$, which means that we can stop. We have τ_i as a product of $2(k_2 - 1) + 1$ transpositions of the desired type. We can do this for all transpositions to get our result. Thus we can generate any permutation in S_n by exchanging adjacent elements. The bubble sort algorithm works this way too, which accepts a permutation then returns the list of n numbers. This is essentially the same problem.

2

We want to find an isomorphism between S_{n-2} and A_n. We define $\varphi : S_{n-2} \to A_n$ thus:

$$\varphi(\sigma) = \begin{cases} \sigma \text{ if } \sigma \text{ is even} \\ \sigma \circ (n-1, n) \text{ if } \sigma \text{ is odd.} \end{cases}$$

We want to see that this is a homomorphism. If both $\sigma, \tau \in S_{n-2}$ are even, then there is nothing to prove. If both are odd, then

$$\varphi(\sigma)\varphi(\tau) = \sigma \circ (n-1, n) \circ \tau \circ (n-1, n) = \sigma \circ \tau = \varphi(\sigma \circ \tau).$$

If σ is odd and τ is even, we have

$$\varphi(\sigma)\sigma(\tau) = \sigma \circ (n-1, n) \circ \tau = \sigma \circ \tau \circ (n-1, n) = \varphi(\sigma \circ \tau).$$

To find the kernel, see that $\varphi(\sigma) = e$ implies that either $\sigma = e$ if σ is even, and if σ is odd, $\sigma \circ (n-1, n)$ can never be the identity element. Thus the kernel is trivial.

This homomorphism restricted to the image gives us an isomorphism of S_{n-2} to a subgroup of A_n.

3

1. For some $1 \leq i \leq n$, $G)i = \{\sigma \in S_n : \sigma(i) = i\} \cong S_{n-1}$. Consider G_i acting on $\{1, 2, \dots, i - 1, i + 1, \dots, n\}$. If $n = 2$, this set will be a singleton, hence trivially transitive. For $n \geq 3$, the set $\{1, 2, \dots, n\} \backslash \{i\}$ has at least two elements. Then $k, \ell \in \{1, 2, \dots, i-1, i+1, \dots, n\}$ such that they are distinct (If $k = \ell$, then $i \in G_i$ works). See that $(k\ell) \in G_i$, as it does not affect i. Then we have $(k\ell)k = \ell$, which means that G_i is transitive.

2. For a doubly transitive action of G on A, let us claim that this action is doubly transitive. Let $B \subseteq A$ be a proper block, then we have elements $b \in B$ and $a \in A \backslash B$. We have $\text{stab}(B) := \{g \in G : gB = B\}$. See that we have $\text{stab}(b) \leq \text{stab}(B)$. To prove this, we consider the map $f : \text{stab}(b) \to \text{stab}(B)$ that sends g to itself. It is evident that $\text{stab}(b) \subseteq \text{stab}(B)$ as sets. Thus we have this relation. So if we have $g \in \text{stab}(b)$, then $gB = B$. Suppose there is an element $c \in B, c \neq b$, by double transitivity of G on A, there is a $\tau \in \text{stab}(b)$ such that $\tau(c) = a$. But then $\tau B \neq B$, a contradiction. Thus either the block is a singleton or the entire set A.

4

Let us denote all elements of Q_8 thus: $1, i, j, k, -1, -i, -j, -k$ are assigned the numbers from 1 to 8. Then see that left multiplication by 1 is the identity permutation on S_8. Left multiplication by i is $(1256)(3478)$, by j is $(1357)(2864)$, and by k is $(1458)(2367)$. Their negatives also have a left regular representation. Now see that i, j can generate Q_8 as a group, then it must stand to reason that their corresponding left regular representations will behave in the same way! Thus, see that $G = \langle (1256)(3478), (1357)(2864) \rangle \cong Q_8$.

5

Consider the action of G on the cosets G/H by left multiplication. $\lambda : G \to S_{|G/H|}$ is the permutation representation of this action, and let K be its kernel. K is normal in G, and we have $K \leq \text{stab}(H) = H$. By the first isomorphism theorem, we have an injective homomorphism $\bar{\lambda} : G/K \to S_{|G/H|}$. Since $|S_{|G/H|}| = n!$, we have $[G : K] \leq n!$.

6

We shall prove a result that for $|G| = n$ and p the smallest prime that divides n, then a subgroup of order p must be normal. Let some $H \leq G$, with $|[G : H]| = p$. Consider the group action of left multiplication on left cosets of H. This group action has a permutation representation, let us denote that by π_H. Take $K = \ker \pi_H$, and $|[H : K]| = k$. Then we have $|[G : K]| = |[G : H]||H : K| = pk$. We know that H has p many left cosets, hence $\frac{G}{K}$ is isomorphic to some subgroup of S_p which is the image of G under π_H. Thus we must have $pk|p! \implies k|(p-1)!$. But since k can only have prime factors greater than or equal to p and $(p-1)!$ has no prime factors greater than p, we must have $k = 1$. Thus $H = K \trianglelefteq G$ is normal.

Let p be the smallest prime dividing n. We know that $p < n$, since n is composite. Then see that there must exist a subgroup of order $\frac{n}{p}$ as given in the problem, hence this subgroup has index $\frac{n}{\frac{n}{p}} = p$, hence this is a normal subgroup. Thus G cannot be simple.

7

We know that $|[G : Z(G)]| = n$. For some $g \in G$, let $\text{Cl}(g)$ be the conjugacy class of g. By orbit stabiliser theorem, we have $|\text{Cl}(g)| = \left|\frac{G}{C_G(g)}\right|$, where $C_G(g)$ is the centraliser. But since $Z(G) \leq C_G(g)$, we have $\left|\frac{G}{C_G(g)}\right| \leq \left|\frac{G}{Z(G)}\right| = n$, which is the required result.

8

Given a permutation $\sigma \in S_n$, let $m_1, \ldots, m_s$ be the distinct integers that appear in the cycle type of σ, including $1-$cycles. Let $k_1, \ldots, k_s$ be the number of times the above cycles appear. Then see that for another $\tau \in S_n$ to be conjugate to it, we must have the exact cycle breakup. For this, we choose a permutation of n integers, then determine where to 'draw' brackets. For each repetition, we factor it out. Then from $n!$, we have for any m_i, and k_i the number of times the cycle of length m_i appears, we get $k_i! m_i^{k_i}$ many such equivalent cycles. For example, (123) and (231) are the same permutation. Thus, we end up with

$$\frac{n!}{(k_1! m_1^{k_1}) \ldots (k_s! m_s^{k_s})}.$$

Take any $\sigma \in S_n$. Then every cycle must be of order p, else the permutation will not have order p. Thus σ consists up any number of $p-$cycles, up to $\lfloor \frac{n}{p} \rfloor$. If σ has k $p-$cycles, its conjugacy must have size

$$\frac{n!}{k! p^k (n - kp)!}.$$

Summing this over all k, we get

$$\sum_{k=0}^{\lfloor \frac{n}{p} \rfloor} \frac{n!}{k! p^k (n - kp)!},$$

the required solution.

9

We know that r is the greatest prime. Then let $n_r = rk+1$ be the number of Sylow $r-$subgroups. Since $rk_1 + 1 | pq$, we can have $rk_1 + 1 = 1, p, q$, or pq. If $rk_1 + 1$ is p or q, it would be absurd to have $k_1 \neq 0$ as for $k_1 = 1$ $r + 1 > p, q$. Assume that $n_r = pq$. Let $qk_2 + 1$ be the number of Sylow $q-$subgroups. Then $qk_2 + 1 = 1, r, pr$. Assume that $n_q = r$. We have $n_p = pk_3 + 1$ as the number of Sylow $p-$subgroups. Then we have $n_p = 1, q, r, qr$. Assume that $n_p = q$. Let us count the number of elements in G of order p, q, r. Since $n_r = pq$, the number of elements of order r is $pq(r-1)$. The number of elements of order q is $(q-1)r$ and the number of elements of order p is $(p-1)q$. Adding these up, for $q > 1$, we have a number that is greater than pqr, which is not possible. Thus at least one of n_p, n_q, n_r is one.

10

We have $|G| = 42 \cdot 11$. Let $n_{11} = 11k+1$ be the number of Sylow $11-$subgroups. Then $11k+1|42$, which essentially forces $k = 0$. As $n_{11} = 1$, there is only one such subgroup which must be normal. Thus G is not simple.