MAT1100HF - HMW 2

Grigorios Fournodavlos
St. No.: 998805761

1. (a) $18 = 2 \cdot 9$. We know that the order of an element $\sigma \in S_n$ is equal to the least common multiple of the orders of the cycles in its cycle decomposition (since cycles without common numbers commute). Thus, the above factorizations of pairwise relatively prime factors of 18 are $n = 18$ or $2 + 9$. It follows that (see (b) for more explanations on the way of thinking) $n = 2 + 9 = 11$ is the least integer required and an element of S_{11} which has order 18 is:

$$\sigma = (12)(34567891011)$$

(b) What we said previously about the order of an element in S_n narrows down a bit our search for a permutation $\sigma \in S_{26}$ of maximal order. Firstly, having more than one cycle of the same type, in the cycle decomposition of σ, does not contribute anything to the order of σ, but can only reduce it (comparing to another choice). If $\sigma_1, \cdots, \sigma_k$ are the cycles corresponding to the structure of σ and $a_1, \cdots, a_k$ their orders, then $a_1 + \cdots + a_k \leq 26$ and $l.c.m.(a_1, \cdots, a_k) = |\sigma|$. We know that the $l.c.m.(a_1, \cdots, a_k)$ is the product of primes to the maximal powers for which each one is a factor of some a_i. This indicates that we can produce larger orders by choosing $a_1, \cdots, a_k$ to be pairwise relatively prime. Actually, it is wiser to choose the orders $a_1, \cdots, a_k$ to be just powers of primes. For example, the choice $a_1 = 2, a_2 = 3, a_3 = 7$ is better than $a'_1 = 2 \cdot 7, a'_2 = 3$, since $l.c.m.(a_1, a_2, a_3) = l.c.m.(a'_1, a'_2) = 42$, but $a_1 + a_2 + a_3 = 12 < 17 = 14 + 3 = a'_1 + a'_2$ which gives us more freedom for adding other cycles to the decomposition of σ (increasing its order). Finally, I think it is more efficient to start with powers of smaller primes and advance to larger ones. Keeping these in mind and playing around a bit I concluded (at least I think so :P) that the maximal order of an element in S_{26} is $2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$ $(2^2 + 3^2 + 5 + 7 = 25)$. One remark, $2^2 \cdot 3^2 \cdot 5 \cdot 7 = 2 \cdot 3 \cdot 5 \cdot 6 \cdot 7$ which would be 7!, if it wasn't missing a 4.

This gives me the sense that for the general case (S_n, perhaps for large n) we should somehow try to achieve the growth of the factorial $m!$ (in the product), instead of that of the exponentials $p_1^{\lambda_1} \cdot \cdots \cdot p_\nu^{\lambda_\nu}$ (with p_i small, i.e. 2,3), because it is both greater and gives a polynomial sum $\frac{m(m+1)}{2}$.

2. Let $H \leq G$ be a subgroup with index $|G : H| = 2$. It follows that $G = H \cup gH$ (partition) for some $g \in G \setminus H$ (such g exists or it would be $G = H$ and $|G : H| = 1$). If $x \in G \setminus H$, then $xH \cap H = \emptyset \;\Rightarrow\; xH = gH$. Also, $Hx \cap H = \emptyset \;\Rightarrow\; Hx = gH \;\Rightarrow\; xH = Hx$ and so H is normal in G.

3. By definition $C_{S_{20}}(\sigma) = \{\tau \in S_{20} \mid \tau\sigma = \sigma\tau\} = \{\tau \in S_{20} \mid \tau^{-1}\sigma\tau = \sigma\}$. If we consider the action of $G \times G \to G$, $g \cdot x = g^{-1}xg = x^g$, for $G = S_{20}$, then $C_{S_{20}}$ is no other than the stabilizer $Stab(\sigma)$. According to the formula $|Stab(\sigma)| = |S_{20}|/|Orb(\sigma)|$, we only have to find the order of the orbit of σ. Note that $Orb(\sigma)$ is the set of all permutations conjugate to σ. Since two permutations are conjugate iff they have the same cycle structure, $|Orb(\sigma)|$ is equal to the number of all permutations of S_{20}, whose cycle decomposition consists of one 5-cycle, two 3-cycles, and one 2-cycle. A simple combinatorial argument shows that the latter equals $\binom{20}{5}4!\binom{15}{3}2!\binom{12}{3}2!\binom{9}{2}1! = \frac{20!}{10!/8} \;\Rightarrow\; |C_{S_{20}}(\sigma)| = |Stab(\sigma)| = 10!/8 = 453,600$.

4. Let G be a group of odd order and suppose there is $g \in G$ such that $x = g^{-1}x^{-1}g$ $\Rightarrow\; x^{-1} = g^{-1}xg$. If m be the order of g, then it is odd since $m \big| |G|$. This fact along with the above relations yield $x = g^{-m}xg^m = x^{-1}$ (formal proof - induction). It follows that $x^2 = e$ and so the order of x is either 1 or 2. Hence, $x = e$, because the order of x divides that of G, which is odd.

5. Assume that $G/Z(G) =< gZ(G) >$. Given $x_1, x_2 \in G$, let $x_1 = g^m y_1$ and $x_2 = g^n y_2$, where $m, n \in \mathbb{Z}$ and $y_1, y_2 \in Z(G)$ (this is possible since G is the union of the cosets $g^j Z(G)$, $j \in \mathbb{Z}$). Since g^m, y_1, g^n, y_2 commute with one another, so do x_1, x_2 and therefore G is Abelian.

6. Suppose that the group of all automorphisms of G, $Aut(G) =< f >$, where f is an automorphism of G. Define $\phi : G/Z(G) \to Aut(G)$, which maps the coset $xZ(G)$ to the inner morphism $g \mapsto g^x$.

   - ϕ is well defined: if $xZ(G) = yZ(G)$, then $g^x = x^{-1}gx = x^{-1}yg^y(x^{-1}y)^{-1} = g^y$, because $x^{-1}y \in Z(G)$.

- ϕ is one to one: let $g^x = g^y \Leftrightarrow x^{-1}gx = y^{-1}gy \Leftrightarrow (yx^{-1})g = g(yx^{-1})$, $\forall g \in G \Leftrightarrow yx^{-1} \in Z(G) \Leftrightarrow xZ(G) = yZ(G)$.

Thus, $G/Z(G) \cong \phi(G/Z(G))$, which is cyclic as a subgroup of the cyclic group $Aut(G)$. Therefore, $G/Z(G)$ is cyclic and by the previous exercise it follows that G is Abelian.

7. (a) Let $H \leq G$ and $(G : H) = n$. Define the action of G on the set of left cosets of H by $(g, xH) \mapsto gxH$. This leads to a morphism $\rho : G \to Sym(\{xH \mid x \in G\}) = S_n$, whose kernel is $ker\rho = \{g \in G \mid gxH = xH, \forall x \in G\} = \{g \in G \mid g(xHx^{-1}) = xHx^{-1}, \forall x \in G\} = \bigcap_{x \in G} xHx^{-1} \leq H$. Of course, $ker\rho \lhd G$ and by the first isomorphism theorem we obtain $G/ker\rho \cong \rho(G) \leq S_n$. More particularly, $(G : ker\rho) < \infty$ and so the normal subgroup $N = ker\rho$ meets our demands.

   (b) Define the map $\phi : \{x(H_1 \cap H_2) \mid x \in G\} \to \{xH_1 \mid x \in G\} \times \{xH_2 \mid x \in G\}$, $\phi(gH_1 \cap H_2) = (gH_1, gH_2)$. First, we notice that this map is well defined. Indeed, if $gH_1 \cap H_2 = hH_1 \cap H_2 \Leftrightarrow g^{-1}h \in H_1 \cap H_2 \Leftrightarrow gH_1 = hH_1$ and $gH_2 = hH_2$. In fact, we have just showed that ϕ is also injective and hence $(G : H_1 \cap H_2) \leq (G : H_1) \cdot (G : H_2) < \infty$.