HW 10

4.4.13

G is partitioned into conjugacy classes where each class has size 1, 7 or 29. The class equation is $203 = |Z(G)| + 7x + 29y$ where x is the number of conjugacy classes of size 7 and y is the number of conjugacy classes of size 29. Since H is a union of conjugacy classes, H cannot contain any element g which belongs in a size-7 class, since then $|H| \geq 8$ (since it contains all the conjugates of g as well as e). Similarly it cannot contain any element which belongs in a size-29 class. Hence $H \leq Z(G)$.

Now $|Z(G)| \geq 7$, and by Lagrange's theorem $|Z(G)|$ is one of $7, 29, 203$. If $|Z(G)| = 7$ then $G/Z(G)$ is order 29, hence cyclic, hence $Z(G) = G$, a contradiction. Similarly $|Z(G)| \neq 29$. Hence $Z(G) = 203$ and G is abelian.

4.4.18a

For $f, g \in G$ let $f \sim g$ if they are conjugates. It suffices to show that $f \sim g \implies \sigma(f) \sim \sigma(g)$, since $\sigma^{-1} \in \mathrm{Aut}(G)$.

If $f \sim g$ there exists $x \in G$ such that $f = xgx^{-1}$; then $\sigma(f) = \sigma(xgx^{-1}) = \sigma(x)\sigma(g)\sigma(x)^{-1}$, hence $\sigma(f) \sim \sigma(g)$.

4.4.18b

Call a member of K' an involution. Any involution has cycles of length 1 or 2, hence the cycle structure must be $2, 2+2, 2+2+2, \ldots$. Here are the values for n for which the longest cycle type possible is $\#(2+2+2)$:

n	#(2)	#(2+2)	#(2+2+2)
2	1	0	0
3	3	0	0
4	6	3	0
5	10	15	0
6	15	45	15
n	$\binom{n}{2}$	$\frac{1}{2!}\binom{n}{2}\binom{n-2}{2}$	$\frac{1}{3!}\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}$

This completes the proof for $n \leq 6$. The general formula is displayed in the last row.

Going from one cell to the one on the right, we multiply by $\frac{1}{2}\binom{n-2}{2}, \frac{1}{3}\binom{n-4}{2}$, etc. This sequence of factors is decreasing, hence a table row is weakly increasing then decreasing (since once a factor becomes less than 1, it will never exceed 1). Hence it suffices to check that $\#(2)$ is less than $\#(2+2)$ and also less than the rightmost nonzero entry in the table.

The first inequalityfollows since $\frac{1}{2}\binom{n}{2}$ is a strictly increasing function for $n > 2$.

For the second inequality, we form a set-embedding f (an injective function) for the two sets in question. Let $f((1,2)) = (12)(34)(56), f(1x) = (12)(xx+1), f(2y) = (12)(yy+1), f(pq) = (12)(pq)$, where $x, y, p, q \notin \{1,2\}$.

For $\sigma \in \mathrm{Aut}(S_n)$ since $\sigma(K)$ must be a conjugacy class of size $|K|$, and furthermore σ preserves orders, we have $\sigma(K) = K$.

4.4.18c

Note that all transpositions are self-inverse. WLOG, we can let $\sigma((1,2)) = (a, b_2)$. Let $\sigma((2,3)) = (p,q)$.

Note that $(2,3)(1,2)(2,3) = (1,3)$, and hence $(p,q)(a,b_2)(p,q) = \sigma((1,3))$.

If $\{p,q\}$ is disjoint from $\{1,2\}$ then the HLS is equal to (a,b_2) which violates the injectivity of σ. Similarly $\{p,q\}$ cannot have two elements in common with $\{a,b_2\}$; hence it has exactly one element in common.

A similar proof shows that σ preserves transposition overlap count (if a,b,c are distinct, then $\sigma((a,b))$ and $\sigma((b,c))$ are transpositions $(p,q),(r,s)$ with exactly one element in common, i.e. $|\{p,q,r,s\}| = 3$).

Hence, if $\sigma((1,2)) = (p,q)$, then $\sigma(1,k)$ has exactly one element in common with $\{p,q\}$ (except for $k = 2$). It suffices to show that this is the same element for all k. Supposing otherwise, assume WLOG $\sigma((1,3)) = (p,q')$ and $\sigma((1,4)) = (p',q)$. Now $(1,3) and (1,4)$ have 1 element in common, but $(p,q'),(p',q)$ do not.

4.4.18d

For arbitrary $1 \leq p < q \leq n$ we have $(1,q)(1,p)(1,q) = (p,q)$. Hence the given set generates all transpositions, hence all of S_n.

Hence any $\sigma \in \mathrm{Aut}(S_n)$ is uniquely determined by its action on $(1,2),\ldots(1,n)$, hence by the distinct values $a, b_2, \ldots b_n$. There are at most $n!$ such possible values.

The map $f : S_n \to \mathrm{Aut}(S_n)$ which maps τ to conjugation by τ is injective since $Z(S_n) = 1$ if $n \geq 3$. Hence there are $n!$ inner automorphisms, which accounts for all $n!$ possible automorphisms.