

## 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  $Z(G) = G$  (by 3.1.36), 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  $\sigma^{-1} \in \text{Aut}(G)$ .

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  $2, 2 + 2, 2 + 2 + 2, \dots$ . 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 inequality follows since  $\frac{1}{2} \binom{n}{2}$  is a strictly increasing function for  $n > 2$ .

For the second inequality, the rightmost nonzero entry is  $\frac{n!}{\frac{n}{2}!2^{\frac{n}{2}}}$  where the division is the division. The ratio of this to  $\#(2)$  is  $\frac{(n-2)!}{\frac{n}{2}!2^{\frac{n}{2}-1}} = \frac{(n-2)(n-3)\dots(\frac{n}{2}+1)}{2^{\frac{n}{2}-1}}$ . The number of factors in the top is  $\lceil \frac{n}{2} \rceil - 2$  and the number of factors at the bottom is  $\lfloor \frac{n}{2} \rfloor - 1$ ; these differ by at most 1. For  $n \geq 6$ , we can thus group them as  $\frac{n-2}{p} \frac{n-3}{2} \frac{n-4}{2} \dots$  where  $p$  is 2 or 4. Each factor is greater than 1 for  $n \geq 6$ .

For  $\sigma \in \text{Aut}(S_n)$  since  $\sigma(K)$  must be a conjugacy class of size  $|K|$ , and furthermore  $\sigma$  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  $\sigma$ . 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  $\sigma$  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, so  $(p, q'), (p', q)$  have one element in common, hence  $p' = q'$ , so  $\sigma((1, 3)) = (p, p'), \sigma((1, 4)) = (q, p')$ . Now by a similar overlap-counting argument,  $(3, 4)$  must be mapped to  $(p, q)$ , but this violates the injectivity of  $\sigma$ .

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

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

#### 4.4.19a

$|K| \neq |K'|$ : this follows by reading off the table in 4.4.18b. Now let  $H \leq \text{Aut}(S_6)$  be defined as  $H = \{\sigma \in \text{Aut}(S_6) : \sigma(K) = K\}$ . Let  $t_1, \dots, t_{15}$  be the transpositions in  $S_6$ , and  $p_1 \dots p_{15}$  be the triple transpositions, and let  $\sigma \in \text{Aut}(S_6)$ . If  $\sigma(t_1) = t_k$  for some  $k$ , then  $\sigma \in H$ . Otherwise  $\sigma(t_1) = p_k$  for some  $k$ , and hence  $\sigma(K) = K'$ , and furthermore  $\sigma(K') = K$ .

If  $H$  is equal to  $\text{Aut}(S_6)$  then  $H$  is index 1. Hence it suffices to show that if there exists some  $\tau \in \text{Aut}(S_6) - H$ , then  $H$  is index 2. For all  $\sigma \in \text{Aut}(S_6)$  either  $\sigma(K) = K$  in which case  $\sigma \in H$  or  $\sigma(K) = K'$  in which case  $\tau\sigma \in H$ . Hence  $\text{Aut}(S_6) = H \sqcup \tau H$  and  $H$  is of index 2.

### 4.4.19b

By repeating 4.4.18c-d,  $|H| = 6!$  and  $H = \text{Inn}(S_6)$  (since every inner automorphism belongs to  $H$ , and there are  $n!$  inner automorphisms).