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 $\sigma^{-1} \in \mathrm{Aut}(G)$.

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 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. The ratio of this to $\#(2)$ is $\frac{(n-2)!}{\frac{n}{2}!2^{\frac{n}{2}-1}} = \frac{(n-2)(n-3)\ldots(\frac{n}{2}+1)}{2^{\frac{n}{2}-1}}$. 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 $\frac{n-2}{p}\frac{n-3}{2}\frac{n-4}{2}\ldots$ where p is 2 or 4. Each factor is greater than 1 for $n \geq 6$.

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, 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 σ.

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.

4.4.19a

$|K| \neq |K'|$: this follows by reading off the table in 4.4.18b. Now let $H \leq \mathrm{Aut}(S_6)$ be defined as $H = \{\sigma \in \mathrm{Aut}(S_6) : \sigma(K) = K\}$. Let $t_1, \ldots t_{15}$ be the transpositions in S_6, and $p_1 \ldots p_{15}$ be the triple transpositions, and let $\sigma \in \mathrm{Aut}(S_6)$. 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 $\mathrm{Aut}(S_6)$ then H is index 1. Hence it suffices to show that if there exists some $\tau \in \mathrm{Aut}(S_6) - H$, then H is index 2. For all $\sigma \in \mathrm{Aut}(S_6)$ either $\sigma(K) = K$ in which case $\sigma \in H$ or $\sigma(K) = K'$ in which case $\tau\sigma \in H$. Hence $\mathrm{Aut}(S_6) = H \sqcup \tau H$ and H is of index 2.

4.4.19b

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

5.1.12a

The image of A in $A \times B$ is $\{(a,e) : a \in a\}$ and the image of A in $A * B$ is $A' = \{(a,e)Z : a \in A\}$. Let $f : A \to A'$ be given by $f(a) = (a,e)Z$. This is a homomorphism since $f(a)f(b) = (a,e)(b,e)Z = (ab,e)Z = f(ab)$. This is surjective by definition.

This is injective. Suppose $f(a) = f(b)$, then $(a,e)Z = (b,e)Z$, then $(a,e)\{x_i, y_i^{-1} : x_i \in Z_1\} = (b,e)\{x_i, y_i^{-1} : x_i : Z_1\}$, then $\{(ax_i, y_i^{-1}) : x_i : Z_1\} = \{(bx_i, y_i^{-1}) : x_i : Z_1\}$. There is only a single tuple in both the LHS and the RHS with e as the second argument, with $y_i = x_i = e$. Hence by comparing the first element of that tuple, $ae = be$, hence $a = b$.

The proof that the image of B is isomorphic to B is similar.

The intersection is $I = \{(ax_i, y_i^{-1})Z : a \in A, x_i \in Z_1\} \cap \{(x_i, by_i^{-1})Z : b \in B, x_i \in Z_1\}$. An element of this intersection is of the form $(ax_i, y_i^{-1})Z = (x_j, bx_j^{-1})Z$ for some $a \in A, b \in B, x_i, \in Z_1, y_j \in Z_2$. This means $(ax_ix_j^{-1}, y_i^{-1}x_jb^{-1}) \in Z$; in particular, $a \in Z_1, b \in Z_2$. Hence $I = \{(ax_i, y_i^{-1})Z : a \in Z_1, x_i \in Z_1\} \cap \{(x_i, by_i^{-1})Z : b \in Z_2, x_i \in Z_1\}$, which is central. This is isomorphic to the intersection of the image of Z_1 and Z_2 in the group $I' = (Z_1 \times Z_2)/Z$ (here Z is understood as a subgroup of $Z_1 \times Z_2$). Hence it suffices to show that the image of Z_1 is the entire group. Let $z_1 \in Z_1, z_2 \in Z_2$ be arbitrary; it is required to show that $(z_1, z_2)Z = (a,e)Z$ for some $a \in Z_1$, or equivalently $(az_1^{-1}, z_2^{-1}) \in Z$. Here we can take $a = z_2'z_1$ where z_2' is the image of z_2 under the isomorphism $Z_1 \cong Z_2$.

$|A * B| = |(A \times B)/Z| = |A||B|/|Z_1|$ since $|Z| = |Z_1|$.

5.1.12b

In $Z_4 * Q_8$ let $X = xZ, I = iZ, j = jZ, k = kZ$. Let ϕ be the set-function $\phi : Z_4 * Q_8 \to Z_4 * Q_8$ be given by $\phi(X) = (x,e)Z, \phi(I) = (e,r)Z, \phi(J) = (x, rs)Z$ where the Z's on the RHS should be understood as the appropriate subgroup of $Z_4 * D_8$.

Since $\{X, I, J\}$ is a generating set, and the image of these forms a generating set of the RHS as well, it suffices to show that this is a group homomorphism.

By considering $Z_4 * Q_8$ as a subgroup of the direct product, it suffices to check the identities $X^4 = I^4 = J^4 = (IJ)^4 = eZ, IJK = X^2$ under the map. First, note that $\phi(K) = (x, r^2s)$.

This becomes $x^4 = e, r^4 = e, (x, rs)^4 = e, (x, r^2s)^4 = e$ and $(x^2, e) = (x^2, rrsr^2s)$.

5.1.14

Let $B = B_1 \times \dots B_n = \{(b_1 \dots b_n) : b_i \in B_i\}, g \in G$. Then $g = (g_1, \dots g_n)$ where $g_i \in A_i$. We have $gB = \{(g_1, \dots g_n)(b_1, \dots b_n) : b_i \in B_i\} = \{(g_1b_1, \dots g_nb_n) : b_i \in B_i\} = \{(b_1'g, \dots b_n'g) : b_i' \in B_i\} \subseteq Bg$ where in the last equality we have used the fact that B_i is normal in A_i. Hence $gB \subseteq Bg$ for all g, which implies B is normal in G.

Let $\phi : G/B \to (A_1/B_1) \times \dots (A_n/B_n)$ be the set-function given by $\phi((g_1, \dots g_n)B) = (g_1B_1, \dots g_nB_n)$. This is well-defined since if $gB = hB$ then comparing elementwise, $g_iB_i = h_iB_i$. We will prove that ϕ is a group isomorphism.

ϕ is a group homomorphism: ϕ maps the identity $(e_1, \dots e_n)B$ to $(e_1B_1, \dots e_nB_n)$, which is the identity in $(A_1/B_1)\times \dots (A_n/B_n)$. Now $\phi((g_1, \dots g_n)B(g'_1, \dots g'_n)B) = \phi((g_1g'_1, \dots g_ng'_n)B) = (g_1g'_1B_1, \dots g_ng'_nB_n) = (g_1B_1, \dots g_nB_n)(g'_1B_1, \dots g'_nB_n) = \phi((g_1, \dots g_n)B)\phi((g'_1, \dots g'_n)B)$. The proof for inverse is similar.

ϕ is surjective: for any element in the codomain $y = (a_1B_1, \dots a_nB_n)$, we can take $g = (a_1, \dots a_n)$ and $\phi(gB) = y$.

ϕ is injective: if $(g_1B_1, \dots g_nB_n) = (h_1B_1, \dots h_nB_n)$ then comparing elementwise, $g_iB_i = h_iB_i$. In the domain it is required to prove that $(g_1, \dots g_n)B = (h_1, \dots h_n)B$, equivalently $(g_1^{-1}, h_1 \dots g_n^{-1}, h_n) \in B$, equivalently $g_i^{-1}h_i \in B_i$, which follows from $g_iB_i = h_iB_i$.