MTH 411: Midterm exam 1
Fall 2015

Problem 1:

Let G be a group. We recall that the set $\mathrm{Aut}(G)$ is the set of all bijective homomorphisms $\phi : G \to G$

1) Show that $\mathrm{Aut}(G)$ is a group for the product operation induced by the composition of maps:

$$\phi\psi = \phi \circ \psi : G \to G$$

If ϕ and ψ are bijective maps $G \to G$, then the composition $\phi \circ \psi$ is a bijective map $G \to G$.
If $g, g' \in G$ then

$$\phi \circ \psi(gg') = \phi(\psi(gg')) = \phi(\psi(g)\psi(g')) = \phi(\psi(g))\phi(\psi(g'))$$

The composition of homorphisms is an homomorphism. The composition satisfies the closure axiom. The associativity of the product follows from the associativity of the composition of maps. The identity map of G is an automorphism, it is the identity element of $\mathrm{Aut}(G)$.
Finally, for any $\phi \in \mathrm{Aut}(G)$, $\phi^{-1} \circ \phi = \phi \circ \phi^{-1} = id_G$ and the inverse map ϕ^{-1} is an automorphism of G: if $g, g' \in G$, we can write $g = \phi(h)$ and $g' = \phi(h')$ as ϕ is surjective, and we have

$$\phi^{-1}(gg') = \phi^{-1}(\phi(h)\phi(h')) = \phi^{-1}(\phi(hh') = hh' = \phi^{-1}(g)\phi^{-1}(g')$$

So any element of $\mathrm{Aut}(G)$ has an inverse.

2) Let $x \in G$ be an element of finite order and $\phi \in \mathrm{Aut}(G)$. Show that $|\phi(x)| = |x|$

For any k, we have $\phi(x^k) = \phi(x)^k$. Thus ϕ sends the subgroup $\langle x \rangle$ of G to $\langle \phi(x) \rangle$. But these subgroups have cardinal $|x|$ and $|\phi(x)|$ and ϕ is bijective. Thus $|x| = |\phi(x)|$.

3) For any $x \in G$ we define a map $i_x : G \to G$ by $i_x(g) = gxg^{-1}$. Show that i_x is an element of $\mathrm{Aut}(G)$.

For any $g, g' \in G$,

$$i_x(gg') = xgg'x^{-1} = (xgx^{-1})(xg'x^{-1}) = i_x(g)i_x(g')$$

so i_x is a homomorphism $G \to G$.
For any $g \in G$

$$i_x(i_{x^{-1}}(g)) = i_x(x^{-1}gx) = xx^{-1}gxx^{-1} = g$$

Similarly, $i_{x^{-1}} \circ i_x = id_G$. Thus i_x is bijective, it is an automorphism of G.

4) Show that the map

$$\begin{array}{cccc} i & : & G & \to & \mathrm{Aut}(G) \\ & & x & \to & i_x \end{array}$$

is an homomorphism of groups.

For $x, x', g \in G$ we have

$$i_{xx'}(g) = (xx')g(xx')^{-1} = x(x'gx'^{-1})x^{-1} = i_x(i_{x'}(g))$$

Thus $i_{xx'} = i_x \circ i_{x'}$: i is a morphism $G \to \mathrm{Aut}(G)$.

5) Prove that the kernel of i is exactly the center $Z(G)$ of G.

Let x such that $i_x = id_G$. Then for any $g \in G$, $i_x(g) = xgx^{-1} = g$ that is $gx = xg$. This is exactly the definition of $x \in Z(G)$. Thus Ker $i = Z(G)$.

The image of the map i is a subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$, called the group of inner automorphisms of G.
6) Show that $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$, where $Z(G)$ is the center of G.

We know that $i : G \to \mathrm{Inn}(G)$ is a surjective homomorphism with kernel $Z(G)$. By the first isomorphism theorem, this means that $\mathrm{Inn}(G) \simeq G/Z(G)$

7) Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Let $x, g \in G$ and $\varphi \in \mathrm{Aut}(G)$. Then

$$\varphi \circ i_x \circ \varphi^{-1}(g) = \varphi(i_x(\varphi^{-1}(g)) = \varphi(x(\varphi^{-1}(g)x^{-1}) = \varphi(x)g\varphi(x^{-1}) = i_{\varphi(x)}(g)$$

Therefore $\varphi \circ i_x \circ \varphi^{-1} = i_{\varphi(x)} \in \mathrm{Inn}(G)$.

Problem 2:
1) For any $\sigma \in S_n$ and $i, j \in \{1, \dots n\}$, show that $\sigma(ij)\sigma^{-1} = (\sigma(i)\sigma(j))$.

Let $k \in \{1, \dots, n$. k is sent to $\sigma^{-1}(k)$ by σ^{-1}. If k is not $\sigma(i)$ or $\sigma(j)$ it is fixed by (ij), and sent back to k by σ. If $k = \sigma(i)$, $\sigma^{-1}(k)$ is sent to $\sigma(j)$ by $\sigma(ij)$.

2)For $i < j \in \{1, \dots, n\}$, compute the permutation

$$(i\ i+1)(i+1\ i+2)\dots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\dots(i\ i+1)$$

We prove it by induction over $j-i$. If $j-i = 2$ then $(j-2\ j-1)(j-1\ j)(j_2\ j-1) = (j-2\ j)$

by question 1).
If $(i+1\ i+2)\dots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\dots(i+1\ i+2) = (i+1 j)$ then

$$(i\,i{+}1)(i{+}1\,i{+}2)\dots(j{-}2\,j{-}1)(j{-}1\,j)(j{-}2\,j{-}1)\dots(i\,i{+}1) = (i\,i{+}1)(i{+}1\,j)(i\,i{+}1) = (ij)$$

by question 1).

3) Conclude that the transpositions $(i\ i+1)$, for $1 \leq i \leq n-1$ generate S_n

The transpositions (ij) for $1 \leq i < j \leq n$ generate S_n. By question 2), these transpositions are all products of transpositions of the $(i\ i+1)$, with $1 \leq i \leq n-1$. Thus this set of permutations also generates S_n.

4) Prove that (12) and the n-cycle $\sigma = (123\dots n)$ generate S_n

By question 1), for $0 \leq k \leq n-1$, we have $\sigma^k(12)\sigma^{-k} = (k+1\ k+2)$. Thus the group generated by (12) and σ contains all transpositions $(i\ i+1)$, and thus these two permutations generate S_n.

5) Using Problem 1, question 2, prove that for $n=4$ or $n=5$, we have $|\mathrm{Aut}(S_n)| \leq \binom{n}{2}(n-1)!$ and conclude that $\mathrm{Aut}(S_4) = \mathrm{Inn}(S_4)$.

Any homomorphism $G \to G$ is determined by its image on a set of generators of G.
By question 2) in Problem 1, for any automorphism ϕ of S_n, the image (12) is an element of order 2 in S_n and the image of σ is an element of order n.
Thus the image of σ is an n-cycle, and there is $\frac{n!}{n} = (n-1)!$ choices for the image, as n-cycles are invariant up to cyclic permutations.
The image of (12) is an element of order in S_4 or S_5, thus it is either a transposition, or a product of two disjoint transpositions.
But A_n is a characteristic subgroup of S_n, thus the image of (12) cannot be a product of two transpositions. So there $\binom{n}{2}$ choices for the image of (12) and $\binom{n}{2}(n-1)!$ total choices.

In the case $n=4$ the bound we get is 36. The group $\mathrm{Inn}(S_4)$ has cardinal $4! = 24$ by question 6) in Problem 1, as the center of S_4 is trivial. Thus the index of $\mathrm{Inn}(S_4)$ in $\mathrm{Aut}(S_4)$ should smaller than $\frac{36}{24}$ so it is 1 and all automorphisms are inner automorphisms.

The bound we would get from this method for S_5 would only give us that $\mathrm{Inn}(S_5)$ has index at most 2 in $\mathrm{Aut}(S_5)$. One can actually show that the index is indeed 2: there is an automorphism of S_5 which is not inner.