MAS 4301 – HW 2

18. Prove that a set with n elements has exactly $n!$ permutations on it.

Proof. We prove a more general result. Suppose A and B are two sets with $|A| = |B| = n$. Then there are exactly $n!$ bijections between A and B.

Base Case: $n = 1$. Suppose $|A| = |B| = 1$. This means that $A = \{a\}$ and $B = \{b\}$. There is in fact only one function from A to B: the one that sends a to b. This function is a bijection. We know that $1! = 1$.

Inductive Case. Suppose that any tie you have two sets both of which have cardinality n then there are exactly $n!$ bijections between the two sets.

Suppose A and B are sets with cardinality $n+1$. Choose $x \in A$ and fix it. Let's denote the set of bijections from A to B by $\mathrm{Bij}(A, B)$. We are going to partition $\mathrm{Bij}(A, B)$ as follows. For each $b \in B$ we let T_b be the set of bijections from A to B that send x to b. Clearly, this forms a partition and therefore

$$|\mathrm{Bij}(A, B)| = \sum_{b \in B} |T_b|.$$

Our aim is to show that $|T_b| = n!$ for each $b \in B$ and so

$$|\mathrm{Bij}(A, B)| = \sum_{b \in B} n! = (n+1)n! = (n+1)!.$$

So fix $b \in B$ and let $A' = A \setminus \{x\}$ and $B' = B \setminus \{b\}$. We should note that $|A'| = |B'| = n$. Take any $f \in T_b$ and observe that the restriction of f to A' is an injection from A' to B'. Conversely, for any $f' \in \mathrm{Bij}(A', B')$ we can extend f' to all of A by taking $f(x) = b$. Then $f \in \mathrm{Bij}(A, B)$. This shows that there is a bijection between the sets T_b and $\mathrm{Bij}(A', B')$. By the inductive hypothesis

$$n! = |\mathrm{Bij}(A', B')| = |T_b|.$$

$\square$

53. Let H be a subgroup of G and $C(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$. Prove $C(H)$ is a subgroup of G. This subgroup is called the *centralizer* of H in G.

Proof. By the definition of identity, we know that $eg = ge$ for all $g \in G$ and equality holds for all $g \in H$. It follows that $e \in C(H)$. Thus, $C(H) \neq \emptyset$. Next, let $x_1, x_2 \in C(H)$. We aim to show that $x_1 x_2 \in C(H)$ and $x_1^{-1} \in H$. To that end, let $h \in H$. Since $H \leq G$ we know that $h^{-1} \in H$ as well.

$$\begin{aligned}(x_1 x_2)h &= x_1(x_2 h) \\ &= x_1(h x_2) \\ &= (x_1 h) x_2 \\ &= h(x_1 x_2).\end{aligned}$$

Since $h \in H$ it follows that $x_1 x_2 \in C(H)$. Next, notice that

$$x_1^{-1} h = (h^{-1} x_1)^{-1} = (x_1 h^{-1})^{-1} = h x_1^{-1}.$$

It follows that $x_1^{-1} \in C(H)$. Therefore, $C(H) \leq G$.

$\square$

54. Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup of G.

Proof. First we note that $e \in H$ since it is a subgroup and $e = geg^{-1} \in gHg^{-1}$. Next, let $x, y \in gHg^{-1}$. Then for some $h_1, h_2 \in H$, $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$. Then

$$\begin{aligned} xy^{-1} &= (gh_1g^{-1})(gh_2g^{-1})^{-1} \\ &= (gh_1g^{-1})((g^{-1})^{-1}h_2^{-1}g^{-1}) \qquad (ab)^{-1} = b^{-1}a^{-1}) \\ &= (gh_1g^{-1})(gh_2g^{-1}) \\ &= g(h_1h_2^{-1})g^{-1} \end{aligned}$$

and this element belongs to gHg^{-1} since H is a subgroup and so $h_1h_2^{-1} \in H$

$\square$

5. We did in class.

6. We construct the subgroups of A_4. We first note that $|A_4| = 12$. Consider the cyclic subgroups of A_4. These are either subgroups of order 2 for the 2,2,-cycles or order 3 for the 3-cycles.

$$< (123) >, < (124) >, < (134) >, < (234) >, < (12)(34) >, < (13)(24) >, < (14)(23) > .$$

It is straightforward to check that the 2,2-cycles commute and so that the subgroup generated by two of them is

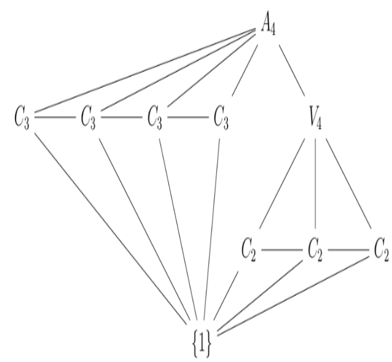
$$V = \{e, (12)(34), (13)(24), (14)(23) > .$$

Notice that there is no subgroup sitting between V and A_4 using the order argument. Any such subgroup would have to have an order which is a multiple of 4 and a divisor of 12... so only 4,12.

We now show that there is no subgroup of order 6. Suppose $K \leq A_4$ and $|K| = 6$. Then we know it cannot contain two of the 2,2 cycles since it would then contain the third one and hence contain V. So it must consist of 3-cycles and at most one 2,2-cycles. It has to contain one of them since the 3 cycles would also get their inverse and some come in pairs with the identity.

So there must exist two 3-cycles and they should have the form $\sigma = (abc)$ and $\tau = (abd)$. (This is in S_4 and so the must share two of the same numbers. Then $\sigma\tau = (a\ c)(b\ d)$ and $\tau\sigma = (a\ d)(b\ c)$ which contradicts that K only has one 2,2-cycle.

Therefore, we have found all of the subgroups of A_4. Here is a picture of the lattice of subgroups of A_4. C_3 denotes a 3-cycle, while C_2 denotes the 2,2-cycles.



13. Let $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m \in S_m$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \ldots, \sigma_m$.

Proof. Suppose σ_i is a k_i-cycle. Since they are disjoint cycles they commute. Also by disjointness, no power of σ_i is a power of σ_j except for the identity. By induction it suffices to show that if g, h commute and the only power of g that is a power of h is the identity, then $|gh| = lcm(|g|, |h|)$.

Set $m = |g|$, $n = |h|$, $r = lcm(m, n)$ and $s = |gh|$. Observe that $(gh)^s = g^s h^s = e$ and so $g^s = h^{-s} = h^{n-s}$. By hypothesis, $g^s = e$ and $h^s = e$, By Proposition 4.12, $n|s$ and $m|s$. Therefore, $r|s$.

Now $r = mk = nj$ for some integers k, j. We know that $g^r = g^{mk} = e$ and $h^r = h^{nj}$. By commutativity

$$(gh)^r = g^r h^r = e.$$

This means that $|gh|$ divides r by Proposition 4.12.

□

Prove that a composition of injective functions is injective. Suppose that $f : A \to B$, $g : B \to C$ are both injective. To show that $(g \circ f)$ is injective we let $a_1, a_2 \in A$ and suppose that $(g \circ f)(a_1) = (g \circ f)(a_2)$. The goal is to show that $a_1 = a_2$.

$$\begin{aligned}
(g \circ f)(a_1) &= (g \circ f)(a_2) \\
g(f(a_1)) &= g(f(a_2)) && \text{(definition of composition)} \\
f(a_1) &= f(a_2) && \text{(since } g \text{ is injective)} \\
a_1 &= a_2 && \text{(since } f \text{ is injective)}
\end{aligned}$$