1. (DF1.1.31) Prove that any group of even order has an element of order 2.

   Proof. Let G be a group of even order, say $2n$ ($n \in \mathbb{Z}^+$). We will show that there is at least one element of order two by showing that the number of elements which do not have order two is strictly less than $2n$.

   First, note that the identity element of G has order 1, so we now have to consider the remaining $2n-1$ elements. When the order of an element g in G is strictly greater than 2, it means that $g^2 \neq 1$, which is the same as saying $g \neq g^{-1}$. And in a similar way we have that $g^{-1} \neq (g^{-1})^{-1}$, so that the order of g^{-1} is strictly greater than 2 as well.

   We can count how many elements in G have orders strictly greater than two by pulling them from G in pairs and identifying two elements at a time in the set $G_{|g|>2} = \left\{g \in G \mid g \neq g^{-1}\right\}$.

   We may scour through the remaining $2n-1$ elements and search for and pick out any element a which has order strictly greater than 2 (if such elements even exist; consider the Klein four-group). If we find an a, we can also pick out a^{-1}, so that they are paired in this way. Both elements have orders greater than 2, so we find these elements in $G_{|g|>2}$. Hence by construction $G_{|g|>2}$ has even cardinality since we could only identify pairs of elements in the set.

   Furthermore, the number of elements in $G_{|g|>2}$ must be strictly less than $2n-1$ since $2n-1$ is odd and if we are picking out pairs of elements we cannot pick all $2n-1$ elements to fit in this set, as there would be at least one element which cannot be paired up at all. Hence the size of the set $G_{|g|>2}$ is less than or equal to $2n-2$.

   Then the number of elements with order 2 is at least $2n-1-(2n-2)=1$, which means there is at least one element of order 2 in a group with even order. $\square$

2. (DF1.1.35) If x is an element of finite order n in a group G, use the Division Algorithm to show that every integral power of x equals one of the elements in the set $\left\{1, x, x^2, \dots, x^{n-1}\right\}$.

   Proof. Let G be a group and let $x \in G$ have finite order n as given. Then consider any integral power of x, say x^k for any $k \in \mathbb{Z}$. From the Division Algorithm, we may write $k = nq + r$, where for every k there exists unique $q, r \in \mathbb{Z}$ such that $0 \leq r < n$. Hence $x^k = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = 1^q x^r$. In the case when q is nonnegative, the last term is equal to x^r, and when q is negative write $q = -p$ where $p \in \mathbb{Z}^+$ (p is a positive integer). Then $1^q = 1^{-p} = (1^{-1})^p = 1^p = 1$, which implies that when q is negative we still end with x^r.

   The integer r by the Division Algorithm may only take on values from 0 to $n-1$, so any integral power of x will take on one of the elements in the set $\left\{x^0, x^1, x^2, \dots, x^{n-1}\right\}$, where of course $x^0 = 1$. $\square$

3. (DF1.3.8) Show that if $\Omega = \{1, 2, 3, \dots\}$ then S_Ω is an infinite group (Do not say $\infty! = \infty$).

   Proof. One way we can show this is to see that $|S_\Omega| \geq |\Omega| = n$ for each n. When n equals 0 or 1 it is clear that S_Ω only contains the trivial map. For every other n, see that at minimum we have n choices to send the first element in the set, and then $n-1$ choices for the next element, and so on. Thus the number of permutaions of these sets is bounded below by n.

Hence in the case where Ω is a countably infinite set, we have a countably infinite number of choices for where we can send the first element to, and then again we have a countably infinite number of choices for the second element, and so on. (So for the cycle $(1\,k)$ for each $k \in \{1,2,3,\dots\}$ there are a countably infinite number of these cycles) This means that S_Ω is also an infinite group whose cardinality is at least $|\Omega|$. $\square$

4. Prove that if $\tau \in S_n$, then for any r-cycle $(a_1a_2\cdots a_r)$, where $r \leq n$, we have

$$\tau(a_1a_2\cdots a_r)\tau^{-1} = (\tau(a_1)\tau(a_2)\cdots\tau(a_r)).$$

This formula is *very useful.*

Proof. Let τ and $(a_1a_2\cdots a_r)$ be elements of S_n as given, and for notational ease let $f \in S_n$ be given by $f = \tau(a_1a_2\cdots a_r)\tau^{-1}$. We can show that this permutation is equal to $(\tau(a_1)\tau(a_2)\cdots\tau(a_r))$ by showing that their actions on elements of S_n agree for all $a_i \in S_n$.

Without loss of generality, instead of computing the action of both permutations on each a_i, we may instead compute the action of each permutation on each $\tau(a_i)$ unambiguously, since τ is a bijection we would be considering the same set of elements a_i but with different labelings (the same set is the image under τ). The following computation is equivalent to showing that $f\tau = \tau(a_1a_2\cdots a_r) = (\tau(a_1)\tau(a_2)\cdots\tau(a_r))\tau$ agree in action for each element a_i.

So consider the set of elements $\{a_1,a_2,\dots,a_n\}$ and its image under τ, $\{\tau(a_1),\tau(a_2),\dots,\tau(a_n)\}$. We may compute the actions of f and $(\tau(a_1)\tau(a_2)\cdots\tau(a_r))$ on each element $\tau(a_i)$ in this second set, and see that they are equal for all i.

In the first case $i > r$ so that the cycle $(a_1a_2\cdots a_r)$ fixes a_i. Then see that

$$\tau(a_1a_2\cdots a_r)\tau^{-1}(\tau(a_i)) = \tau((a_1a_2\cdots a_r)(\tau^{-1}(\tau(a_i)))) = \tau((a_1a_2\cdots a_r)(a_i)) = \tau(a_i),$$

which means that overall the permutation f fixes $\tau(a_i)$, which is in agreement with the action of $(\tau(a_1)\tau(a_2)\cdots\tau(a_r))$ on $\tau(a_i)$ since $i > r$.

Then in the other case where $i \leq r$ so that the cycle $(a_1a_2\cdots a_r)$ does not fix a_i, see that

$$\tau(a_1a_2\cdots a_r)\tau^{-1}(\tau(a_i)) = \tau((a_1a_2\cdots a_r)(\tau^{-1}(\tau(a_i)))) = \tau((a_1a_2\cdots a_r)(a_i)) = \tau(a_{i+1 \pmod r}).$$

Again this is in agreement with how $(\tau(a_1)\tau(a_2)\cdots\tau(a_r))$ will map $\tau(a_i)$ to $\tau(a_{i+1 \pmod r})$ when $i \leq r$.

So both permutations f and $(\tau(a_1)\tau(a_2)\cdots\tau(a_r))$ agree in action for all elements $\tau(a_i)$ and so they must be equal. $\square$