Instructions: Do any four of the seven problems. Don’t forget to put your name on your answer sheets.

1. Let $G$ be a cyclic group. Let $S$ be the union of all of the proper subgroups of $G$.
   
   (a) If $G$ is infinite, show that $|G - S| = 2$ (i.e., show that there are only two elements in $G$ that are not in $S$).
   
   (b) If $G$ is finite, show that $|G - S| = \phi(|G|)$ (i.e., show that there are $\phi(|G|)$ elements in $G$ that are not in $S$).
   
   (c) Prove that a cyclic group $G$ is never a union of proper subgroups.

   **Answer:** (a) If $G = \langle g \rangle$ is an infinite cyclic group, then it has only two generators: $g$, which is given, and $g^{-1}$. Clearly, any subgroup that has either $g$ or $g^{-1}$ has the other, so one generates if and only if the other does. But if $n$ is an integer but not either 1 or $-1$, then $g^n > g^{-1}$ can’t contain $g$, since then $(g^n)^m = g$ implies $(g^{nm}) = e_G$, and hence that $g$, and so $G$, has finite order. A similar argument shows that $< g >$ can’t contain $g^{-1}$.

   Every element $x \in G$ that is not a generator of $G$ is in $S$, since $< x >$ is a proper subgroup. Thus $G - S = \{g, g^{-1}\}$, so $|G - S| = 2$.

   (b) As in (a), $G - S$ is the set of elements of $G$ which are generators of $G$; if $G$ is a finite cyclic group of order $n$, then it is isomorphic to $\mathbb{Z}_n$, and hence has $\phi(n)$ generators. So $|G - S| = \phi(n)$.

   (c) Since $|G - S| > 0$, we see that $G$ is never the union $S$ of its proper subgroups.

2. Let $G$ be a group.
   
   (a) Let $F$ and $H$ be subgroups of $G$, and assume that $F$ does not contain $H$ and that $H$ does not contain $F$. Let $f$ be an element of $F$ that is not in $H$ and let $h$ be an element of $H$ that is not in $F$. Show that $fh$ is not in either $F$ nor $H$ (i.e., show that $fh$ is not in $F \cup H$).
   
   (b) Show that $G$ is not the union of any two proper subgroups.

   **Answer:** (a) If $fh \in F$, then $fh = g$ for some $g \in F$, so $h = f^{-1}g \in F$, contradicting our assumption. Similarly, if $fh \in H$, then $f \in H$, which is a contradiction. This means that $fh$ is in neither $F$ nor $H$.

   (b) Say $G$ were the union of two proper subgroups; call them $F$ and $H$. If $F \subset H$, then $G = F \cup H = H$, which contradicts $H$ being proper. Likewise, we can’t have $H \subset F$. Thus neither of $F$ and $H$ contains the other, so there is an $f \in F - H$ and an $h \in H - F$, so $fh$ is in neither $F$ nor $H$, which means that $G$ can’t be the union of $F$ and $H$.

3. Let $F, F_1, \ldots$ be the Fibonacci sequence (thus $F_0 = 1, F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for every $n \geq 1$). Prove that $F_n \geq 1.5^n$ for all $n \geq 5$.

   **Answer:** Clearly, $F_5 = 8 \geq 8(243/256) = 243/32 = 1.5^5$, and $F_6 = 13 \geq 12(243/256) = 1.5^6$. And if $F_k \geq 1.5^{k}$ and $F_{k-1} \geq 1.5^{k-1}$ for some $k \geq 6$, then $F_{k+1} = F_k + F_{k-1} \geq 1.5^k + 1.5^{k-1} = 1.5^{k-1}(2.5) > 1.5^{k-1}(2.25) = 1.5^{k+1}$. Now $F_5 \geq 1.5^5$ for all $n \geq 5$ follows by induction.

4. Prove that $Z_{12} \oplus Z_{30}$ is isomorphic to $Z_{60} \oplus Z_6$, but not to $Z_{24} \oplus Z_{15}$.

   **Answer:** First, by the Chinese Remainder Theorem, $Z_{12} \oplus Z_{30} \cong Z_{12} \oplus Z_{5} \oplus Z_{6} \cong Z_{12} \oplus Z_{5} \oplus Z_{6} \cong Z_{60} \oplus Z_6$. But no element of $Z_{12} \oplus Z_{30}$ has order more than 60, since 60 is the lcm of 12 and 30, whereas $(1, 1) \in Z_{24} \oplus Z_{15}$ has order 120, so $Z_{12} \oplus Z_{30}$ is not isomorphic to $Z_{24} \oplus Z_{15}$.

5. Let $f: G \to H$ be a homomorphism of groups.
   
   (a) Define the kernel of $f$.
   
   (b) Prove that the kernel of $f$ is a subgroup of $G$.
   
   (c) Prove that the kernel of $f$ is a normal subgroup of $G$.

   **Answer:** (a) ker $f = \{x \in G | f(x) = e_H\}$

   (b) Since $e_G \in$ ker $f$, we know ker $f$ is not empty. If $x, y \in$ ker $f$, then $f(xy) = f(x)f(y) = e_He_H = e_H$, so $xy \in$ ker $f$, so ker $f$ is closed under the group operation. And if $x \in$ ker $f$, then $f(x^{-1}) = (f(x))^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in$ ker $f$, hence ker $f$ is closed under taking inverses. Thus ker $f$ is a subgroup.

   (c) Let $x \in$ ker $f$ and let $g \in G$. Then $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)e_Hf(g)^{-1} = f(g)f(g)^{-1} = e_H$, so $gxg^{-1} \in$ ker $f$, hence ker $f$ is normal.

6. Let $n > 1$ be a positive integer.
   
   (a) Prove that the number of elements of order $n$ in $S_n$ is at least $(n-1)!$. [Hint: look at n-cycles.]
   
   (b) Prove that $S_n$ has an element of order $n$ that is not an n-cycle if and only if $n$ is not a power of a prime.

   **Answer:** (a) There are $n!$ ways to write down an n-cycle (since this is the number of ways of ordering the numbers 1 to $n$). But these can be grouped into sets of n orderings which define the same n-cycle, so there are $n!/n = (n-1)!$ n-cycles in $S_n$.

   (b) If $n$ is not a power of a prime, then we can factor $n$ so that $n = km$, where $1 < k < m < n$, gcd($k$, $m$) = 1, but $n = km$. Now $k + m < 2m \leq km = n$, so we can find a disjoint $k$-cycle (call it $\sigma$) and m-cycle (call it $\tau$) in $S_n$. Then $\sigma \tau$ has order $n$, since $n$ is the lcm of $k$ and $m$. Conversely, assume $S_n$ has an element $\tau$ of order $n$ but that $\tau$ is not an n-cycle. If $\tau$ is a cycle, it must be an r-cycle with $r < n$, but then it has order $r < n$. Thus $\tau$ is a product of disjoint cycles, and the lcm of the lengths of the cycles is $n$. If $n$ were a power of a prime, then since each length divides $n$, the lengths are powers of the prime. Thus the lcm is the length which is the largest power, but all of the lengths are less than $n$, so the order would be less than $n$, contrary to assumption. Thus $n$ can’t be a power of a prime.