Problem 1:

We proceed by induction.

First, note that $O(S_1) = 1$ (there is only one map on a set with one element, and it is bijective.)

Next, assume that for all $n \leq N$, $O(S_n) = n!$.

Consider the set $\{1, 2 \dots N+1\}$. There are $N+1$ ways to omit a single point, S, from this set; there are $N!$ bijective functions from the set $1, 2 \dots N$ to the set $\{1, 2 \dots N+1\} \setminus \{S\}$. For each such function,f there is a unique bijective function, ϕ_f from $\{1, 2 \dots N+1\}$ to $\{1, 2 \dots N+1\}$ such that $\phi_f(n) = f(n)$ if $n \leq N$; it is given by $\phi_f(n) = f(n)$ if $n \leq N$ and $\phi_f(N+1) = S$.

So there are $N!(N+1)$ bijective functions from $\{1, 2 \dots N+1\}$ to $\{1, 2 \dots N+1\}$.

That is, $O(S_{N+1}) = (N+1)!$.

Thus, for all $n \in \mathbb{N}$, $O(S_n) = n!$.

Problem 2:

Let G be a group and $H \subset G$ be nonempty and finite.

If $H < G$, then if $a \in H$ and $b \in H$, then $ab \in H$. Else, H does not inherit the group operation of G.

Next, assume that $a, b \in H$ implies that $ab \in H$.

Then H inherits the group operation of G.

Because the group operation of G was associative, the inherited group operation on H is also associative.

Further, $e \in H$:

Because H is nonempty, there is an element, a, in H. So, let $a \in H$

A quick proof by induction shows that for all $n \in \mathbb{N}$, $a^n \in H$.

Yet, H is finite. So, there is a pair, $n, m \in \mathbb{N}$ with $n \neq m$ such that $a^n = a^m$.

Now, $a^{|n-m|} \in H$. Also, $a^{|n-m|} = e$, by the cancellation theorem proven in class. Note for future work that this also means that for all $a \in H$, there is an $l \in \mathbb{N}$ such that $a^l = e$.

So $e \in H$.

Next, for all $a \in H$, $a^{-1} \in H$:

Let $a \in H$.

From the above work, there is an $l \in \mathbb{N}$ such that $a^l = e$.

If $l = 1$, then $a = a^{-1}$.

Else, define $b = a^{l-1}$. From earlier work, $b \in H$. Also, $ab = ba = a^l = e$.

So $b = a^{-1}$; a has an inverse in H.

Thus, H is a group under the inherited group operation of G: $H < G$.

So $H < G$ if and only if for all $a, b \in H$, $ab \in H$.

Problem 3:

Let G be a group such that for all $a, b \in G$ and for three given consectuve integers i, $(ab)^i = a^i b^i$.

Then there is an $n \in \mathbb{Z}$ such that for all $a, b \in G$:

$$\begin{aligned}(ab)^n &= a^n b^n \\ (ab)^{n-1} &= a^{n-1} b^{n-1} = a^{-1}(ab)^n b^{-1} \\ (ab)^{n+1} &= a^{n+1} b^{n+1} = a(ab)^n b\end{aligned}$$

Now, for all $a, b \in G$,

$$\begin{aligned}ab &= (ab)^n((ab)^{n-1})^{-1} \\ &= a^n b^n b((ab)^n)^{-1} a \\ &= a^n b^n b((ab)^n)^{-1} a \\ &= a^{-1} a^{n+1} b^{n+1}((ab)^n)^{-1} a \\ &= a^{-1}(ab)^{n+1}(ab)^{-n} a \\ &= a^{-1}(ab)a \\ &= a^{-1}aba \\ &= ba\end{aligned}$$

To summarize, for all $a, b \in G$, $ab = ba$. That is, G is abelian.

Problem 4:

Let $G = \langle \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \rangle < GL_2(\mathbb{R})$.

G has 8 elements; they are:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Now, consider $D_4 = \langle r, s \rangle$, where r is a rotation by 90 degrees and s is a reflection.

Let $\phi : G \to D_4$ be given as follows:

$$\begin{aligned}
\phi(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}) &= r, \\
\phi(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}) &= r^2, \\
\phi(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}) &= r^3, \\
\phi(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) &= e, \\
\phi(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}) &= s, \\
\phi(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}) &= sr, \\
\phi(\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}) &= sr^2, \\
\phi(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}) &= sr^3.
\end{aligned}$$

Then it is readily checked (where "readily" means "it takes not more than 64 matrix multiplications", and I can write code to do that) that ϕ is a homomorphism. It is clear that ϕ is both one-to-one and onto, so that ϕ is a bijection. That is, ϕ is an isomorphism.

Problem 5:

As described, Q_8 has at least 8 elements:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}.$$

However, Q_8 does not have any more elements, as is readily checked ("readily" as above).

Moreover, Q_8 is not isomorphic to D_4; D_4 has only 2 distinct elements of order 4 (r and r^3). However, Q_8 has at least 4 distinct elements of order 4 (both generators and their inverses).

Problem 6:

Let G be a cyclic group, and $H < G$.

Then $G = \langle a \rangle$ for some $a \in G$.

If $|H| = 1$, then H is generated by e.

Else, there is a least positive $n \in \mathbb{N}$ such that $a^n \in H$.

Now, assume there is an $m \in \mathbb{N}$ such that $a^m \in H$ and $m \neq ln$ for all $l \in \mathbb{N}$.

Then $m = qn + r$ for some r between 1 and $n - 1$ (inclusive).

So $a^m a^{-qn} \in H$. But $a^m a^{-qn} = a^{qn+r-qn} = a^r$, and $r < n$. This is contrary to n being the "least" positive such value.

So there is no $m \in \mathbb{N}$ such that $a^m \in H$ and $m \neq ln$ for all $l \in \mathbb{N}$.

That is, for all $m \in \mathbb{N}$ such that $a^m \in H$, $m = ln$ for some $l \in \mathbb{N}$.

So $H = \langle a^n \rangle$. So H is cyclic.

So any subgroup of a cyclic group is cyclic.