Abstract Algebra hw4

Chengyu Hsieh, B13201053

1) (a) We assume that (b) is proven and use its proof and result. We have

$$|\mathbb{Z}/p\mathbb{Z}| = p \quad \text{and} \quad |\mathbb{Z}/q\mathbb{Z}| = q$$

Note that both $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ are cyclic.
Since $(p, q) = 1$, the direct product of the groups, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, is also cyclic, with $(1, 1)$ as its generator. Its order is the product of the individual orders:

$$|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}| = pq$$

The order of $\mathbb{Z}/pq\mathbb{Z}$ is also pq:
Since both $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/pq\mathbb{Z}$ are cyclic groups of the same order pq, they are isomorphic. Now, the map ϕ that sends the generator of the direct product to the generator of $\mathbb{Z}/pq\mathbb{Z}$:

$$\phi : (1, 1) \mapsto 1$$

is clearly an isomorphism.

(b) Assume that $G \times H$ is cyclic. Let (g, h) generate $G \times H$. Let $(|G|, |H|) = k$, $|G| = ck$, $|H| = dk$. Then $[|G|, |H|] = cdk$. Clearly, $(g, h)^{cdk} = (e, e)$. Since (g, h) is the generator, we must have $cdk \geq |G \times H| = |G||H| = cdk^2$. But also $cdk \leq cdk^2$ so $cdk = cdk^2$ and hence $k = 1$.
Now assume that $(|G|, |H|) = 1$. Let g generate G and h generate H. Then for any i such that $(g, h)^i = (e, e)$, we must have $|G| \mid i$ and $|H| \mid i$. From this we have $|G||H| = [|G|, |H|] \mid i$ and $i \geq |G||H| = |G \times H|$. Also note that $(g, h)^{|G||H|} = (e, e)$. Hence (g, h) fullfill the properties of a generator for the group, and so $G \times H$ is cyclic.

(c) The proper subgroups of S_3 are $\{e, r, r^2\}$, $\{e, s\}$, $\{e, rs\}$, $\{e, r^2 s\}$ and e. All of those proper subgroups are cyclic, and by (b) if S_3 is a direct product of some of its proper subgroup then it should be cyclic, but S_3 is not cyclic and hence it cannot be a direct product of any of its proper subgroups.

2) $G = \{e, a, a^2, a^3, a^4, a^5, b, ba, ba^2, ba^3, ba^4, ba^5\}$, which has order 12. See that ba has order 4. However the elements in H can only be of order $1, 2, 3, 6$. Hence the two groups are not isomorphic.

3) (a) Orbit of $\langle(12)\rangle$ is $\{\{1, 2\}, \{3\}, \{4\}\}$.
Orbit of $\langle(123)\rangle$ is $\{\{1, 2, 3\}, \{4\}\}$.
Orbit of V is $\{\{1, 2, 3, 4\}\}$.

(b) $\langle(1234)\rangle$ has the same orbit.

(c) Suppose that $s \in Z(S_4)$. $((12)s)(3) = ((12)s(12))(3) = s(3)$. Hence $s(3) \neq 1, 2$. Similarily, using $(14), (24)$ we obtain that $s(3) \neq 1, 2, 4$. Hence $s(3) = 3$. Similarily we obtain $s(i) = i$ for $i = 1, 2, 3, 4$, therefore s is the trivial permutation. We conclude that $Z(S_4)$ is trivial.

4) (a) For any $g \in G$, $s_1, s_2 \in S$, if $g(s_1) = g(s_2)$ then $s_1 = g^{-1}g(s_1) = g^{-1}g(s_2) = s_2$, hence $g(\cdot)$ is injective. Also for any $s \in S$, $g(g^{-1}(s)) = s$, hence $g(\cdot)$ is surjective. We conclude that $g(\cdot)$ is bijective and may generate a permutation of S. Let $\phi : G \to \mathrm{Perm}(S)$ be defined as $\phi(g) =$ the permutation generated by $g(\cdot)$. Now for any $s \in S$, $g, h \in G$,

$$
\begin{aligned}
&g(h(s)) = (gh)(s) \\
\Rightarrow &\phi(g)\phi(h) = \phi(gh)
\end{aligned}
$$

Hence ϕ is a homomorphism.

(b) If $\phi(g') = \phi(e)$, then $\phi(g')(H) = H$. Then we have $g'H = H$ and hence $g' \in H$. We conclude that the kernel of ϕ is in H.

(c) Note that $|S| = |G|/|H| = n$. Hence $S_n \simeq \mathrm{Perm}(S)$. From (b) we know that $\ker\phi \subseteq H$. But $\ker\phi$ is a normal subgroup of G, and adding the condition that (c) gives we see that $\ker\phi$ must be trivial, meaning that ϕ is injective. We now define $\phi' : G \to \mathrm{Im}(\phi)$ by $\phi'(g) = \phi(g)$. Then ϕ' is clearly an isomorphism. Hence G is isomorphic to a subgroup of S_n.