1. (3 points each) Give examples of the following, if they exist. Otherwise briefly explain why such examples do not exist.

   (a) A group G of order at least 3 such that the only subgroups of G are e and G.
   $\mathbb{Z}_p$ for $p \geq 3$ a prime

   (b) A group G with two elements $a, b \in G$ such that $|a| < \infty$ and $|b| = \infty$
   $G = \mathbb{Z}$, $a = 0$, $b = 1$

   (c) A non-cyclic Abelian group.
   $G = U(8)$

   (d) An element of order 15 in S_8.
   $(123)(45678)$

   (e) An infinite, noncyclic group.
   $GL(2, \mathbb{R})$

   (f) Two nonisomorphic groups of order 18.
   $\mathbb{Z}_{18}$ and D_9

2. (16 points) Consider the permutation group S_8, and let $\sigma = (13256)(23)(78)(46512)$.

   (a) Express σ as a product of disjoint cycles.
   $(124)(35)(6)(78)$

   (b) Express σ as a product of transpositions.
   $(14)(12)(35)(78)$

   (c) Give, in disjoint cycle notation, the element σ^{101}.
   Since $|\sigma| = 6$ and $101 = 6 \cdot 16 + 5$, $\sigma^{101} = \sigma^5 = \sigma^{-1} = (142)(35)(6)(78)$

3. (16 points) Consider the cyclic group G of order 24 generated by a. (So $G = \langle a \rangle$.)

   (a) State a necessary and sufficient condition for an element a^k to generate G.
   $\gcd(24, k) = 1$

   (b) State explicitly all generators of G.
   $a,\ a^5,\ a^7,\ a^{11},\ a^{13},\ a^{17},\ a^{19},\ a^{23}$

   (c) Use Fundamental Theorem of Cyclic Groups to give the orders of all subgroups of G.
   Since G is cyclic, we know $k \mid 24$ if and only if G contains a subgraph of order k. Thus, G contains subgroups of order 1, 2, 3, 4, 6, 8, 12, and 24.

4. (20 points)

(a) State the definition of a *group*.
A group is a set G and a binary operation on G such that

i. the operation is closed $\big(\forall a, b \in G, ab \in G\big)$,
ii. the operation is associative $\big(\forall a, b, c \in G,\ a(bc) = (ab)c\big)$,
iii. there exists an identity element $\big(\exists e \in G$, such that $\forall g \in G\ ge = eg = g\big)$, and
iv. every element has an inverse $\big(\forall g \in G,\ \exists h \in G$, such that $gh = hg = e\big)$.

Note that because the definition of *binary operation* implies closure, you technically do not have to include that though I usually do anyway....

(b) Let G be an Abelian group and let H be the subset of elements of finite order from G. Prove that $H \leq G$.

(I will use the two-step subgroup theorem.)

Let G be an Abelian group and let H be the subset of elements of finite order from G. Since $|e| = 1$, we know $e \in H$. So H is nonempty. ✓

Let $a, b \in H$. Then $|a| = m$ and $|b| = n$ for some $m, n \in \mathbb{Z}$. Now

$$\begin{aligned}(ab)^{mn} &= a^{mn}b^{mn} && \text{since } G \text{ is Abelian}\\ &= (a^m)^n(b^n)^m && \text{properties of exponents}\\ &= e^n e^m && \text{since } |a| = m \text{ and } |b| = n\\ &= e.\end{aligned}$$

Thus $|ab| \leq mn$ and we know $ab \in H$.✓

Finally, we know that $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$. So $a \in H$ implies $a^{-1} \in H$. ✓

[Observe that this is Example 6 on page 63.]

5. (20 points)

(a) State the definition of a *group isomorphism*.
Let G and $\overline{G}$ be groups. The function $\phi : G \to \overline{G}$ is an isomorphism if

i. ϕ is a bijection, and
ii. ϕ is operation preserving $\big(\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)\big)$.

(b) Let G be a group. Show that $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is an isomorphism if and only if G is Abelian.

Proof: ($\Longrightarrow$:) Assume $\phi(g) = g^{-1}$ is an isomorphism. Then for all $a, b \in G$, we know

$$\begin{aligned} b^{-1}a^{-1} &= (ab)^{-1} && \text{by Socks and Shoes} \\ &= \phi(ab) && \text{by the definition of } \phi \\ &= \phi(a)\phi(b) && \text{since } \phi \text{ is order preserving} \\ &= a^{-1}b^{-1} && \text{by the definition of } \phi. \end{aligned}$$

Now, multiply both sides of $b^{-1}a^{-1} = a^{-1}b^{-1}$ on the left by ab and on the right by ba, we obtain, $ab(b^{-1}a^{-1})ba = ab(a^{-1}b^{-1})ba$ which simplifies to $ab = ba$. Since a and b were arbitrary, we have shown that G is Abelian.

($\Longleftarrow$:) Assume G is abelian.
(ϕ is one-to-one) Assume there exist $a, b \in G$ such that $\phi(a) = \phi(b)$. Then by the definition of ϕ, $a^{-1} = b^{-1}$. Operate on the left by a and the right by b, we obtain $b = a$. So ϕ is one-to-one.
(ϕ is onto) Let $a \in G$. Then $a^{-1} \in G$. Now $\phi(a^{-1}) = a$. Thus ϕ is onto.
(ϕ is operation preserving) Let $a, b \in G$. Now,

$$\begin{aligned} \phi(ab) &= (ab)^{-1} && \text{by the definition of } \phi \\ &= b^{-1}a^{-1} && \text{by Socks and Shoes} \\ &= a^{-1}b^{-1} && \text{since } G \text{ is Abelian} \\ &= \phi(a)\phi(b) && \text{by the definition of } \phi. \end{aligned}$$

Thus, we have shown that ϕ is operation preserving.

6. (10 points) Prove that every group of order 4 is Abelian.

Proof: (by contradiction) Assume $a, b \in G$ and $ab \neq ba$. Then, neither a nor b can be the identity, which commutes with all elements. Further, a and b are not inverses of each other, since these too commute. (i.e. $aa^{-1} = a^{-1}a$) Thus, ab and ba must be distinct from e, a, b and each other. So $|G| \geq 5$, a contradiction.

Proof: (direct) If G is cyclic, then G is Abelian. So, assume G has order 4 and is not cyclic. Let $a \in G - e$. Since G is not cyclic, there exists $b \in G$ such that $b \notin \langle a \rangle$. Since G is a group, $ab \in G$ and $ba \in G$. But neither ab nor ba can be elements of $\langle a \rangle$ because $b \notin \langle a \rangle$. Thus we know $G = \{e, a, b, ab, ba\}$. It is now sufficient to show that $ba = ab$. A case analysis shows the other possibilities are impossible:

$ba = e$ implies $b = a^{-1} \in \langle a \rangle$
$ba = a$ implies $b = e \in \langle a \rangle$
$ba = b$ implies $a = e$