1. (D&F 1.1.22, 25, 32) **Orders.** Let $G$ be a group and let $x \in G$.

(a) If $g \in G$, show $|g^{-1}xg| = |x|$ and deduce that $|ab| = |ba|$ for all $a, b \in G$.

(b) Prove that if $|x| \leq 2$ for all $x \in G$ then $G$ is abelian.

(c) If $|x| = n < \infty$, prove that the elements $e, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

2. (D&F 1.1.24) If $a, b \in G$ commute, show (by induction on positive $n$ first) that $(ab)^n = a^n b^n$.

3. (D&F 1.1.28, 30) **Direct Products.** As defined in Example 6 on page 18, if $(A, *)$ and $(B, \diamond)$ are groups, we can form a new group $A \times B$, called their direct product, whose elements are those in the Cartesian Product $A \times B = \{(a, b) \mid a \in A, b \in B\}$ and whose operation is defined component-wise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \ast a_2, b_1 \diamond b_2).$$

For example, if $A = B = \mathbb{R}$ and $\ast = \diamond = +$, then $\mathbb{R} \times \mathbb{R}$ is the familiar $\mathbb{R}^2$.

(a) Verify the group axioms for $A \times B$ (see exercise 28 on p. 22).

(b) Prove that the elements $(a, 1)$ and $(1, b)$ commute and deduce that the order of $(a, b)$ is the least common multiple of $|a|$ and $|b|$ (you can use problem 2).

(c) Show that the direct product is commutative and associative, i.e. that (1) $A \times B \cong B \times A$, and (2) if $G = A \times B$ and $H = B \times C$, then $G \times C \cong A \times H$.

4. (D&F 1.2.1, 2, 7, 10) **The dihedral group.** The dihedral group $D_{2n}$ has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

(a) Compute the order of each of the elements in $D_8$.

(b) Use the generators and relations above to show that if $x$ is any element of $D_{2n}$ which is not a power of $r$, then

$$rx = xr^{-1} \quad \text{and} \quad |x| = 2.$$
forms and alternative presentation of $D_{2n}$ (you have to show that $S = \{s_1, s_2\}$ generates the whole group and that you can derive these relations from the old ones and vice versa).

(d) Consider a cube in $\mathbb{R}^3$, and let $G$ be the group of rigid motions of the cube (motions which fix the unlabeled cube, but possibly move the labeled cube). Following the argument on p. 24 for $D_{2n}$, show $|G| = 24$.

5. The symmetric group.

(a) Let $\sigma$ be the permutation

$$1 \mapsto 2 \quad 2 \mapsto 4 \quad 3 \mapsto 3 \quad 4 \mapsto 1$$

and $\tau$ be the permutation

$$1 \mapsto 2 \quad 2 \mapsto 1 \quad 3 \mapsto 4 \quad 4 \mapsto 3.$$  

Compute the cycle decompositions of $\sigma$, $\tau$, $\sigma^2$, $\tau^2$, $\tau\sigma$, $\sigma\tau$, and $\sigma^2\tau$.

Determine the orders of $\sigma$, $\tau$, and $\sigma\tau$ (not using the claim stated in class).

(b) Let

$$\alpha = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7), \quad \beta = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12), \quad \text{and} \quad \gamma = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8).$$

(i) Compute $\alpha^2$, $\beta^2$, and $\gamma^2$.

(ii) For which $i$ between 1 and 7 is $\alpha^i$ still a 7-cycle? ... between 1 and 12 is $\beta^i$ still a 12-cycle? ... between 1 and 8 is $\gamma^i$ still an 8-cycle?

(iii) What’s the theorem in general?

If $\sigma$ is an $m$-cycle, then $\sigma^i$ is also an $m$-cycle if and only if ...

(Just state, don’t prove it.)

(c) Prove that if $\sigma$ is the $m$-cycle $(a_1 \ a_2 \ldots \ a_m)$, then for all $i = 1, \ldots, m$,

$$\sigma^i(a_k) = a_{\overline{k+i}}$$

where $\overline{k+i}$ is the least residue mod $m$.

Deduce that $|\sigma| = m$.

(d) Use the last part and problem 2 to prove that the order of an element in $S_n$ equals the least common multiple of the lengths of the cycles in its cycle decomposition (you may assume that disjoint cycles commute).

(e) Which values appear as orders of elements of $S_5$ (for which $i$ is there some element of $S_5$ that has order $i$)? For each value, give an example of an element that has that order.

6. Homomorphisms and subgroups.

(a) Which of the following subsets are subgroups?

(i) $\{a + ai \mid a \in \mathbb{R}\} \subseteq \mathbb{C}$, (ii) $\{(i \ j) \mid (i \ j) \in S_n\} \subseteq S_n$, (iii) $\{\text{odd integers}\} \subseteq \mathbb{Z}$ (under +)

(b) Let $\varphi : G \to H$ be a homomorphism of groups. Show that the kernel of $\varphi$ (all elements of $G$ which map to $e_H$) is a subgroup of $G$. 
(c) Show that the maps
\[ \varphi, \psi : G \rightarrow G \] defined by \[ \varphi : g \mapsto g^{-1} \] and \[ \psi : g \mapsto g^2 \]
are homomorphisms if and only if \( G \) is abelian. For each map, give an example of a group \( G \) for which the map is an isomorphism and a group \( H \) for which the map is not an isomorphism (briefly justify).

(d) Prove that if \( H \) and \( K \) are subgroups of \( G \), then so is \( H \cap K \).
On the other hand, prove \( H \cup K \) is a subgroup if and only if \( H \subseteq K \) or \( K \subseteq H \).