1. Short Answer (8 points each)

(a) Draw the subgroup lattice for $Q_8$.

(b) Find the order of $30$ in $\mathbb{Z}/54\mathbb{Z}$.
Since $\overline{30} = 30 \overline{1}$, Proposition 5 (Chapter 3) gives $|\overline{30}| = 30 \overline{1} = \frac{54}{\gcd(54,30)} = \frac{54}{6} = 9$.
Computing directly, $\langle 30 \rangle = \{0, 30, 6, 36, 12, 42, 18, 48, 24\}$.

(c) State the class equation.
Let $g_1, g_2, \ldots, g_k$ be representatives from the conjugacy classes of $G$ that have more than one element. Then

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|.$$

(d) Write down the elements of a Sylow 2-subgroup of $A_4$.
$V = \{1, (12)(34), (13)(24), (14)(23)\}$

(e) Give an example of a non-abelian group that is simple.
The smallest example is $A_5$. 
2. Suppose $n \geq 3$. Show that the set $A = \{ x \in D_{2n} \mid x^2 = 1 \}$ is not a subgroup of $D_{2n}$.

Consider the usual notation $D_{2n} = \{ 1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1} \}$.

Certainly we have $1^2 = 1$ and $s^2 = 1$, but also observe that

$$(sr^k)^2 = (sr^k)(sr^k) = (sr^k)(r^{-k} s) = sr^k r^{-k} s = ss = 1.$$ 

This gives us at least $n + 1$ elements $1, s, sr, sr^2, \ldots, sr^{n-1}$ whose square is 1. Now, not every element of $D_{2n}$ has 1 as a square, since $r^2 \neq 1$.

Therefore $n + 1 \leq |A| < 2n$. If $A$ were a subgroup, its order would have to divide $|D_{2n}| = 2n$, but that’s impossible because $n < |A| < 2n$. Conclusion: $A$ is not a subgroup.

3. Prove the multiplicative group $\mathbb{Q}^+$ of positive rational numbers is generated by the set $A = \left\{ \frac{1}{p} \mid p \text{ is prime} \right\}$.

**Proof:** First we are going to show that any reciprocal $\frac{1}{m}$ of a positive integer $m$ is a product of powers of elements of $A$. Let $m$ have prime factorization $m = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}$. Then

$$\frac{1}{m} = \left( \frac{1}{p_1} \right)^{x_1} \left( \frac{1}{p_2} \right)^{x_2} \cdots \left( \frac{1}{p_k} \right)^{x_k}$$

is a product of powers of elements of $A$, so it belongs to $\langle A \rangle$. Similarly, if $n = p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k}$, then

$$n = \left( \frac{1}{p_1} \right)^{-y_1} \left( \frac{1}{p_2} \right)^{-y_2} \cdots \left( \frac{1}{p_k} \right)^{-y_k}$$

so it follows that any positive integer belongs to $\langle A \rangle$.

Finally, consider an arbitrary $\frac{n}{m} \in \mathbb{Q}^+$. Because $n, \frac{1}{m} \in A$ (as established above), we have $\frac{n}{m} = n \frac{1}{m} \in \langle A \rangle$. This shows $\mathbb{Q}^+ \leq \langle A \rangle$. On the other hand, it is obvious that $\langle A \rangle \leq \mathbb{Q}^+$. Therefore $\mathbb{Q}^+ = \langle A \rangle$. ■
4. Prove that if $G/Z(G)$ is cyclic, then $G$ is abelian.

**Proof:** Suppose $G/Z(G)$ is cyclic.
Then for some $a \in G$ we have $G/Z(G) \cong \langle aZ(G) \rangle = \{Z(G), aZ(G), a^2Z(G), a^3Z(G), \ldots, a^nZ(G)\}$, with $a^nZ(G) = Z(G)$. Because the cosets in $G/Z(G)$ form a partition of $G$, any two elements $x, y \in G$ can be written as $x = a^kz_1$ and $y = a^\ell z_2$ for appropriate powers $k, \ell$ and $z_1, z_2 \in Z(G)$. Then

$$xy = (a^kz_1)(a^\ell z_2) = a^kz_1a^\ell z_2 = a^k a^\ell z_1 z_2 = a^\ell a^k z_2 z_1 = (a^\ell z_2)(a^k z_1) = yx.$$ 

Therefore $G$ is abelian. ■

5. Prove that if $|G : H| = 2$, then $H \leq G$.

**Proof:** Suppose $|G : H| = 2$. Let $a \in G - H$ so the left-cosets of $H$ are precisely $H$ and $aH$. Now, it is necessarily the case that $aH = G - H$, because there are just two cosets, and any element not in $H$ must be in the other coset $aH$, and conversely.

Similarly, for right cosets we have $Ha = G - H = aH$. This establishes $Ha = aH$, or rather $H = aHa^{-1}$ for all $a \in G - H$. On the other hand, if $a \notin G - H$, then $a \in H$ and $H = aHa^{-1}$ trivially.

We’ve now reasoned that $H = aHa^{-1}$ for all $a \in G$. Thus $H \leq G$. ■
6. Prove that characteristic subgroups are normal.

**Proof:** Suppose $H$ is characteristic in $G$.
This means that $\varphi(H) = H$ for any $\varphi \in \text{Aut}(G)$.
Given $g \in G$, let $\varphi_g \in \text{Aut}(G)$ be the inner automorphism $\varphi_g(x) = gxg^{-1}$.
Then $\varphi_g(H) = H$, which means $gHg^{-1} = H$.
It follows that $H$ is normal.

7. Prove that a group of order 56 has a normal Sylow $p$-group for some prime $p$ dividing its order.

**Proof:** As $56 = 2^3 \cdot 7$, the only primes dividing its order are 2 and 7. Thus we seek a normal Sylow 2-subgroup $P$ (of order $2^3 = 8$), or a normal Sylow 7-subgroup $Q$ (of order 7).

Let $Q \in \text{Syl}_7(G)$. If $n_7 = 1$, then $Q \trianglelefteq G$, in which case we are done. Otherwise, assume $n_7 > 1$. Sylow’s theorem asserts $n_7 = 1 + 7k$, for some integer $k$, and $n_7|8$. The only possibility is $n_7 = 8$.

Let the 8 Sylow 7-groups be $\{Q_1, Q_2, Q_3, \ldots, Q_8\}$, with $Q_1 = Q$. If $i \neq j$, then $Q_i \cap Q_j$ is a proper subgroup of $Q_i \cong Z_7$, so $Q_i \cap Q_j = 1$. Thus the sets $Q_i - \{1\}$ are disjoint. Let $X = \bigcup_{i=1}^{8} (Q_i - \{1\})$, so $|X| = 8 \cdot 6 = 48$. Any element of $X$ is a non-identity element of some $Q_i \cong Z_7$, and therefore has order 7. Note that $G$ has exactly $56 - 48 = 8$ elements that are not in this union, and one of these elements is 1. Say $G - X = \{1, g_1, g_2, g_3, \ldots g_7\}$.

Now, consider a Sylow 2-subgroup $P$, for which $|P| = 2^3 = 8$. As no element of $P$ has order 7, it is necessarily the case that $P = \{1, g_1, g_2, g_3, \ldots g_8\}$. This is the only possibility for $P$, so we conclude that $P$ is the unique Sylow 2-subgroup, hence $P$ is normal.

In conclusion, either $Q$ or $P$ is normal.