1. Given a group, define its center (Zentrum):
   \[ Z(G) := \{ g \in G : gh = hg \text{ for all } h \in G \}. \]
   Note that \( Z(G) \) is abelian and \( Z(G) \trianglelefteq G \). If \( G/Z(G) \) is cyclic, show that \( G \) is abelian.

   **Proof.** Assume that \( G/Z(G) \) is cyclic. Then we have \( G/Z(G) = \langle gZ(G) \rangle \) for some coset \( gZ(G) \), which means that every coset has the form \( g^iZ(g) \) for some \( i \in \mathbb{Z} \). Since the cosets partition \( G \), every element of \( G \) has the form \( g^iz \) for some \( i \in \mathbb{Z} \) and \( z \in Z(G) \). Finally, consider any two elements \( g^iz_1 \) and \( g^jz_2 \) of \( G \), with \( i, j \in \mathbb{Z} \) and \( z_1, z_2 \in Z(G) \). Then we have
   \[ g^iz_1g^jz_2 = g^ig^iz_1z_2 = g^{i+j}z_1z_2 = g^ig^jz_1z_2 = g^jg^i z_2z_1 = g^jz_2g^iz_1z_2. \]
   Hence \( G \) is abelian. \( \square \)

2. Let \( p \) be prime and consider a group \( G \) of order \( p^2 \).
   (a) Use the class equation to show that \( p \) divides \( |Z(G)| \).
   (b) Use Problem 1 to show that \( G \) must be abelian.
   (c) Show that \( G \) must be isomorphic to \( \mathbb{Z}/p^2 \) or \( \mathbb{Z}/p \times \mathbb{Z}/p \).

   **Proof.** Suppose that \( |G| = p^2 \), where \( p \) is prime, and let \( G \) act on itself by conjugation. That is, consider the homomorphism \( \alpha : G \to \text{Aut}(G) \) defined by \( \alpha_g(h) := ghg^{-1} \) for all \( g, h \in G \).
   Given \( x \in G \), the orbit \( \text{Orb}(x) \) is called a conjugacy class and the stabilizer \( C(x) := \text{Stab}(x) \) is called the centralizer. By the Orbit-Stabilizer theorem we have \( |\text{Orb}(x)| = |G|/|C(x)| \). Note also that \( |\text{Orb}(x)| = 1 \) if and only if \( x \in Z(G) \). Then since \( G \) is a disjoint union of conjugacy classes \( G = \bigcup_i \text{Orb}(x_i) \), we can write
   \[ |G| = \sum_i |\text{Orb}(x_i)| = \sum_i |G|/|C(x_i)| = |Z(G)| + \sum_{C(x_i) \neq G} |G|/|C(x_i)|. \]
   This is called the class equation. If \( C(x_i) \neq G \) then we have \( |C(x_i)| = 1 \) or \( |C(x_i)| = p \) by Lagrange. In either case we see that \( p \) divides \( |G|/|C(x_i)| \). Since \( p \) also divides \( |G| \), we conclude from the class equation that \( p \) divides \( |Z(G)| \). This implies that \( |G|/|Z(G)| = 1 \) or \( |G|/|Z(G)| = p \). In either case, we see that \( G/Z(G) \) is cyclic, so Problem 1 implies that \( G \) is abelian.

   For all \( 1 \neq x \in G \), the order \( |x| \) divides \( p^2 \). If \( G \) has an element of order \( p^2 \), then \( G \) is isomorphic to the cyclic group \( \mathbb{Z}/p^2 \). So suppose that every nonidentity element of \( G \) has order \( p \). Choose \( 1 \neq x \in G \) and define \( H := \langle x \rangle \leq G \). Then choose \( y \in G - H \) and define \( K := \langle y \rangle \leq G \). We claim that \( G \approx H \times K \). Indeed, since \( G \) is abelian we only need to check that \( H \cap K = 1 \) and \( HK = G \). Suppose \( H \cap K \neq 1 \). Then since \( |H \cap K| \) divides \( p \) we conclude that \( |H \cap K| = p \) and hence \( H = H \cap K = K \). This contradicts the fact that \( y \in G - H \). Thus \( H \cap K = 1 \). Applying the counting formula gives
   \[ |HK| = \frac{|H||K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2, \]
   and it follows that \( HK = G \). We conclude that \( G \approx H \times K = \langle x \rangle \times \langle y \rangle \approx \mathbb{Z}/p \times \mathbb{Z}/p \). \( \square \)
3. Let $p > 2$ be prime. Prove that every group of order $2p$ is either cyclic or dihedral.

**Proof.** Suppose that $|G| = 2p$, where $p > 2$ is prime. By Cauchy’s Theorem $G$ has an element of order 2, say $x \in G$, and an element of order $p$, say $y \in G$. Note that $|\langle x \rangle \cap \langle y \rangle|$ divides $|\langle x \rangle| = 2$ and $|\langle y \rangle| = p$, hence $|\langle x \rangle \cap \langle y \rangle| = 1$. Then we have

$$|\langle x \rangle \langle y \rangle| = \frac{|\langle x \rangle||\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = \frac{2 \cdot p}{1} = 2p,$$

hence $\langle x \rangle \langle y \rangle = G$. Since $\langle y \rangle$ has index 2, it is normal (we could also use Sylow’s theorem to show this) and we conclude that $G = \langle x \rangle \ltimes \langle y \rangle$. It remains to see how $\langle x \rangle$ acts on $\langle y \rangle$ by conjugation.

Since $\langle y \rangle$ is normal, note that $xyx^{-1} = xy = y^i$ for some $i \in \mathbb{Z}$. Then we have

$$y = x^2yx^2 = x(xy)x = xyx(\cdots)(xy) = y^iy^\cdots y^i = y^{i^2},$$

hence $y^{i^2-1} = 1$. This means that $p$ divides $i^2 - 1 = (i + 1)(i - 1)$ and since $p$ is prime this implies $p$ divides $i - 1$ or $p$ divides $i + 1$. If $p$ divides $i - 1$, then $xyx = y^i = y^{i+1}y^{-1}y = 1 = y = y$, hence $G$ is abelian. We conclude that $G$ is cyclic:

$$G = \langle x \rangle \ltimes \langle y \rangle \approx \mathbb{Z}/2 \times \mathbb{Z}/p \approx \mathbb{Z}/(2p).$$

If $p$ divides $i + 1$, then $xyx = y^i = y^{i+1}y^{-1} = 1y^{-1} = y^{-1}$, and we conclude that $G$ is dihedral:

$$G = \langle x \rangle \ltimes \langle y \rangle \approx D_{2p}.$$

\[\square\]

4. Prove that the alternating group $A_4$ is not simple.

**Proof.** Let $V \subseteq A_4$ be the subset containing the identity and all elements of the form $(ij)(k\ell)$:

$$V := \{1, (12)(34), (13)(24), (14)(23)\}.$$

Recall that any permutation has order equal to the least common multiple of the lengths of its cycles. Thus the non-identity elements of $V$ all have order 2. Note that $V$ is a **subgroup** of $A_4$ because

$$[(12)(34)][(13)(24)] = (14)(23),$$

$$[(12)(34)][(14)(23)] = (13)(24),$$

$$[(13)(24)][(14)(23)] = (12)(34).$$

Finally, recall that conjugation of permutations preserves the cycle structure. This implies that $V$ is a union of conjugacy classes, and hence is **normal**. \[\square\]

[I mentioned in class that the special orthogonal groups are almost simple. In particular, for odd $n$ the group $SO(n)$ is simple and for even $n$ (except 4) the group $SO(n)/\{\pm I\}$ is simple. The anomalous fact that $SO(4)$ is not simple should be related to the anomalous fact that $A_4$ is not simple. However, I do not know a direct link between them.]

5. If $|G| = 30$, prove that $G$ is not simple.

[I will give two proofs. The first answers this specific question and the second proves the more general fact that if $|G| = pqr$ with $p < q < r$ prime, then $G$ is not simple.]
Proof 1. Suppose that $|G| = 30 = 2 \cdot 3 \cdot 5$. Let $P$ be a Sylow 5-subgroup and let $Q$ be a Sylow 3-subgroup. Note that $P \cap Q = 1$ since every element of the intersection has order dividing 3 and dividing 5. Note also that $|PQ| = |P||Q|/|P \cap Q| = 3 \cdot 5/1 = 15$. If we knew that one of $P$ or $Q$ is normal, this would imply that $G$ is not simple.

So suppose that $P$ and $Q$ are both non-normal and let $n_5$ and $n_3$ be the numbers of Sylow 5-subgroups and Sylow 3-subgroups, respectively. Since $P$ and $Q$ are non-normal we have $n_5 > 1$ and $n_3 > 1$. By Sylow’s theorem we know that $n_5|6$ and $n_5 = 1 \pmod{5}$, which implies $n_5 = 6$. We also know $n_3|10$ and $n_3 = 1 \pmod{3}$, which implies $n_3 = 10$. How could there be so many Sylow subgroups? There can’t, and here’s why. Note that any element of order 5 in $G$ generates a Sylow 5-subgroup. Furthermore, every Sylow 5-subgroup is cyclic and so it is generated by any non-identity element. Thus any two Sylow 5-subgroups must intersect trivially. It follows that $G$ contains exactly $6 \cdot 4 = 24$ elements of order 5. By similar reasoning, $G$ contains $10 \cdot 2 = 20$ elements of order 3. But $24 + 20 = 44 > 30 = |G|$. This contradiction proves that one of $P$ or $Q$ must be normal. \(\Box\)

Proof 2. Suppose that $|G| = pqr$ with $p < q < r$ prime. Let $n_r, n_q, n_p$ be the numbers of Sylow $r$-subgroups, $q$-subgroups and $p$-subgroups, respectively. If any of $n_r$, $n_q$ or $n_p$ equals 1 then we obtain a normal Sylow subgroup, so assume that $n_r, n_q, n_p > 1$. Then by Sylow’s theorem we have $n_r = pq$, $n_q \in \{r, pr\}$ and $n_p \in \{q, r, qr\}$. Note that the Sylow subgroups are all cyclic and intersect trivially. By counting the group elements of order $r, q, p$, and 1, we find that

$$pqr = |G| \geq pq(r-1) + r(q-1) + q(p-1) + 1 = pqr + (r-1)(q-1).$$

This implies $0 \geq (r-1)(q-1)$, which contradicts the fact that $(r-1) > 0$ and $(q-1) > 0$. \(\Box\)

[Yes, that proof was a bit too slick.]