1. *Let G be a finite group whose order is greater than 2 but not divisible by 4. Prove that G contains an element of odd order (other than the identity).*

   Proof. There are two possible cases we should address, both of which are fairly straightforward.

   Case I: G has odd order. Then, by a simple consequence of Lagrange's Theorem, every element of G has order which divides the order of G, and since an odd number has no even divisors, every element of G has odd order.

   Case II: G has even order. Let $|G| = 2k$, where k is odd (we know k is odd because the order of G is not divisible by 4). The orders of elements of G are thus, by Lagrange's theorem, divisors of $2k$. If any non-identity element has odd order, we're done; if any element g has order 2ℓ for $\ell > 2$, then since $\ell | k$, ℓ is odd and g^2 will have order ℓ. Thus, the only circumstance we need to address is the possibility that *every non-identity element* in G has order 2. Let us suppose that to be the case, and derive a contradiction.

   Since $|G| > 2$, G contains at least the identity element e and two distinct non-identity elements a, and b; the latter two, by our assumption, have order 2, so $a = a^{-1}$ and $b = b^{-1}$. In addition, ab will have order 2, so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Thus, $\{e, a, b, ab\}$ will be a subgroup of G, and so by Lagrange's theorem the order of G must be divisible by 4, which contradicts our premise. □

2. *Let G be an Abelian group of order 15. Prove that G is cyclic.*

   Proof. By Lagrange's Theorem, every element of G has order divisible by 15, i.e., the possible orders of elements of G are 1, 3, 5, and 15. We know exactly one element, the identity, has order 1, and if any elements have order 15, then we are done, since any such element would generate the whole group. Let us consider the possibilities where G only contains elements of order 3 and 5.

   Case I: Every non-identity element of G is of order 3. Let a and b be distinct non-identity elements such that $a^2 \neq b$. Since G is Abelian and each of a, b, and ab has order 3, it is easy to list out all the elements generated by a and b. So $\{e, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2\}$ is a subgroup of G, and since that group has 9 elements, Lagrange's Theorem requires that $9 \mid 15$, which is a contradiction.

   Case II: Every non-identity element of G is of order 5. Consider some non-identity element a and the subgroup $H = \langle a \rangle = \{e, a, a^2, a^3, a^4\}$ which it generates. Consider some $b \notin H$; b also has order 5, so let us consider the cosets H, bH, b^2H, b^3H, and b^4H. Since H has index 3, at least two of these four cosets must be the same, so that $b^kH = b^\ell H$ for some distinct k, ℓ from 0 to 5. By the equlity criterion for cosets, $b^{k-\ell} \in H$, but $b^{k-\ell} \neq e$, so some generator of H is a power of b, and so b generates H, contradicting our assumption that $b \notin H$.

   Case III: G contains at least one element of order 3 and at least one element of order 5. Let a have order 3 and b have order 5. A brute force (or number-theoretic) argument indicates that since $(ab)^k = a^kb^k$, this power equals the identity only when $3 \mid k$ and $5 \mid k$; i.e., when $15 \mid k$, so ab would have order 15. □

3. *Suppose $|G| = p^2$ with p prime. For non-identity elements a and b of G, prove that if $\langle a \rangle \neq \langle b \rangle$, then every element of the group can be expressed in the form a^kb^ℓ for integers k and ℓ.*

   By Lagrange's Theorem, every subgroup of G has order 1, p, or p^2; in particular $\langle a \rangle$ and $\langle b \rangle$ must have those orders, and since a and b are nonidentity elements, they do not generate subgroups of order 1. If either subgroup (WLOG $\langle a \rangle$) has order p^2, then $\langle a \rangle = G$ and every element of G can be written in the form a^kb^0. Thus the only interesting case is when $\langle a \rangle$ and $\langle b \rangle$ both have order p.

   Note that any non-identity element of a group of prime order generates the whole group, so since $\langle a \rangle \neq \langle b \rangle$, these two groups do not overlap at all except in the identity element. Thus, since $b^k \notin \langle a \rangle$

except when $b^k = e$, we may assert that the cosets $\langle a\rangle, \langle a\rangle b, \langle a\rangle b^2, \dots, \langle a\rangle b^{p-1}$ are all distinct and disjoint, and thus account for all p^2 elements of G. Since every element of G lies in one of these cosets, every element of G may be written as a power of a times a power of b.

4. *Recall that the* center $Z(G)$ *of a group G is the subgroup whose elements are of the form $\{x \in G : xa = ax$ for all $a \in G\}$. Prove that $Z(G_1 \oplus G_2) = Z(G_1) \oplus Z(G_2)$; that is, that the center of a direct product is the direct product of centers.*

   Proof. We shall start by showing that every element of $Z(G_1 \oplus G_2)$ is in $Z(G_1) \oplus Z(G_2)$. Let (x_1, x_2) be an element of $Z(G_1 \oplus G_2)$; this element is characterized by the fact that $(x_1, x_2)(a_1, a_2) = (a_1, a_2)(x_1, x_2)$ for all $(a_1, a_2) \in G_1 \oplus G_2$. Performing the direct-product multiplication on both sides of this criterion, we get that $(x_1a_1, x_2a_2) = (a_1x_1, a_2, x_2)$. Since two elements of a direct product group are equal only if each term is equal, then we require that $x_1a_1 = a_1x_1$ and $x_2a_2 = a_2x_2$ for any $(a_1, a_2) \in G_1 \oplus G_2$, which is to say, any $a_1 \in G_1$ and $a_2 \in G_2$. Since $x_1a_1 = a_1x_1$ for any $a_1 \in G_1$, $x_1 \in Z(G_1)$; likewise $x_2 \in Z(G_2)$. Thus this $(x_1, x_2) \in Z(G_1) \oplus Z(G_2)$.

   Conversely, let (x_1, x_2) be an element of $Z(G_1) \oplus Z(G_2)$. By the construction of a direct product, $x_1 \in Z(G_1)$ and $x_2 \in Z(G_2)$, and thus $x_1a_1 = a_1x_1$ for any $a_1 \in G_1$, and $x_2a_2 = a_2x_2$ for any $a_2 \in G_2$. Assembling these two equalities into a pairwise equality of coordinates, our criterion is that, considered as elements of $G_1 \oplus G_2$, $(x_1a_1, x_2a_2) = (a_1x_1, a_2x_2)$ for any $a_1 \in G_1$ and $a_2 \in G_2$. Rewriting this in terms of the product of elements of $G_1 \oplus G_2$, our criterion will be that $(x_1, x_2)(a_1, a_2) = (a_1, a_2)(x_1, x_2)$ for any $(a_1, a_2) \in G_1 \oplus G_2$. In other words, (x_1, x_2) must commute with any element of $G_1 \oplus G_2$, and is thus an element of $Z(G_1 \oplus G_2)$. □

5. *Prove that $S_3 \oplus Z_2$ is isomorphic to D_6; you may find it helpful to define a specific isomorphism.*

   Let us define an isomorphism from D_6 to $S_3 \oplus Z_2$. We would want to map r to some element of $S_3 \oplus Z_2$ of order 6; such an element mught be the product of an element of S_3 of order 3 (i.e. one of the two 3-cycles) with an element of Z_2 of order 2 (the number 1), so we select $\phi(r) = ((123), 1)$. We then want f to be associated with some element of order 2; which one won't matter much, as long as we map it to a different element than we map r^3 to. We might choose, for instance, $\phi(f) = ((12), 1)$. This induces the rest of the isomorphism:

$$\begin{aligned}
\phi(e) &= (e, 0)\\
\phi(r) &= ((123), 1)\\
\phi(r^2) &= ((132), 0)\\
\phi(r^3) &= (e, 1)\\
\phi(r^4) &= ((123), 0)\\
\phi(r^5) &= ((132), 1)\\
\phi(f) &= ((12), 1)\\
\phi(fr) &= ((23), 0)\\
\phi(fr^2) &= ((13), 1)\\
\phi(fr^3) &= ((12), 0)\\
\phi(fr^4) &= ((23), 1)\\
\phi(fr^5) &= ((13), 0)
\end{aligned}$$