Problem (Problem 1)**:** Show that every element of order 2 in A_n is the square of an element of order 4 in S_n.

Solution: Let $\alpha \in A_n$ be written as a product of disjoint cycles

$$\alpha = \sigma_1 \cdots \sigma_r,$$

such that $\alpha^2 = e$. Since $\alpha = \alpha^{-1}$, we then have that

$$\alpha = \sigma_1^{-1} \cdots \sigma_r^{-1},$$

whence each of $\sigma_1, \dots, \sigma_r$ is of order 2. In particular, this means that α is in fact a product of an even number of disjoint transpositions, which we will rewrite as

$$\alpha = \tau_1 \cdots \tau_{2k}.$$

Pairing up these transpositions, we observe that

$$\begin{aligned}\tau_1\tau_2 &= (a_1, b_1)(a_2, b_2)\\ &= (a_1, a_2, b_1, b_2)^2,\end{aligned}$$

whence we have k 4-cycles $\zeta_1, \dots, \zeta_k$ given by

$$\zeta_i^2 = \tau_{2i-1}\tau_{2i}$$

Each of these ζ_i are disjoint, of order 4, and we have

$$\gamma = \zeta_1 \cdots \zeta_k$$

is of order 4 in S_n and is such that

$$\gamma^2 = \alpha.$$

Problem (Problem 2)**:** Let $G = \langle x \rangle$ be a cyclic group, H an arbitrary group. Let $\varphi_1, \varphi_2 \colon G \to \operatorname{aut}(H)$ be homomorphisms such that $\operatorname{im}(\varphi_1)$ and $\operatorname{im}(\varphi_2)$ are conjugate. If G is infinite, also assume that φ_1 and φ_2 are injective. Prove that the semidirect products $H \rtimes_{\varphi_1} G$ and $H \rtimes_{\varphi_2} G$ are isomorphic.

Solution: Let $M_1 = \varphi_1(G)$ and $M_2 = \varphi_2(G)$. We start with the assumption that φ_1 and φ_2 are injective and that G is infinite. It then follows that $M_1 = \langle \varphi_1(x) \rangle$ and $M_2 = \langle \varphi_2(x) \rangle$ by injectivity. Since M_1 and M_2 are conjugate, it follows that there is some $g \in \operatorname{aut}(H)$ such that $gM_1g^{-1} = M_2$. Conjugation is an isomorphism, so this means that $g\varphi_1(x)g^{-1} = \varphi_2(x)^\ell$ for some integer ℓ. Yet, since G is infinite, it must be the case that $\ell = 1$.

Define the map $\psi \colon H \rtimes_{\varphi_1} G \to H \rtimes_{\varphi_2} G$ by taking

$$(x, y) \mapsto (g(x), y),$$

where g is the automorphism discussed earlier. Since g is an automorphism, it follows that ψ is a bijection of sets, so we only need to show that it is a homomorphism, which we do below:

$$\begin{aligned}\psi((x_1, y_1)(x_2, y_2)) &= \psi(x_1\varphi_1(y_1)(x_2), y_1y_2)\\ &= (g(x_1)g(\varphi_1(y_1)(x_2)), y_1y_2)\\ &= (g(x_1)\varphi_2(y_1)(g(x_2)), y_1y_2)\\ &= (g(x_1), y_1) \cdot (g(x_2), y_2).\end{aligned}$$

Now, suppose G is of finite order. Via a similar process, we observe that there is $g \in \operatorname{aut}(H)$ such that $g\varphi_1(x)g^{-1} = \varphi_2(x)^a = \varphi_2(x^a)$ for some $a \in \mathbb{Z}$. Observe that $\gcd(a, m) = 1$, where m is the order of the image of G under both φ_1 and φ_2. If a is already coprime to n, then $\langle x^a \rangle = G$. Else, we use the fact established via the Chinese Remainder Theorem that the surjection $[w]_n \rightarrow [w]_m$ induces a surjection from $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ whenever $m|n$. In particular, this means there is some $a' \in \mathbb{Z}/n\mathbb{Z}$ such that $a' \equiv a$ modulo m and $\gcd(a', n) = 1$.

Define the map

$$\begin{aligned}\Psi\colon H \rtimes_{\varphi_1} G &\rightarrow H \rtimes_{\varphi_2} (G)\\ (x, y) &\mapsto \left(g(x), y^{a'}\right).\end{aligned}$$

Since $G = \langle x \rangle = \left\langle x^{a'} \right\rangle$ and g is an automorphism, it follows that Ψ is a bijective set map, so all we need to verify is that Ψ is a group homomorphism. This can be seen by taking

$$\begin{aligned}\Psi((x_1, y_1) \cdot (x_2, y_2)) &= \Psi(x_1 \varphi_1(y_1)(x_2), y_1 y_2)\\ &= \left(g(x_1) g\varphi_1(y_1)(x_2), y_1^{a'} y_2^{a'}\right)\\ &= \left(g(x_1)\varphi_2(y_1)^a g(x_2), y_1^{a'} y_2^{a'}\right)\\ &= \left(g(x_1)\varphi_2\left(y_1^a\right) g(x_2), y_1^{a'} y_2^{a'}\right)\\ &= \left(g(x_1)\varphi_2\left(y_1^{a'}\right) g(x_2), y_1^{a'} y_2^{a'}\right)\\ &= \left(g(x_1), y_1^{a'}\right) \cdot \left(g(x_2), y_2^{a'}\right)\\ &= \Psi(x_1, y_1) \cdot \Psi(x_2, y_2).\end{aligned}$$

Problem (Problem 3)**:**

(a) Construct a nonabelian group of order 75.

(b) Show that up to isomorphism there are three groups of order 75.

Solution:

(a) We observe that $75 = 3 \cdot 5^2$, so by the result on subgroups of the form $p^2 q$, with $q < p$, we have a unique 5-Sylow subgroup. Suppose this 5-Sylow subgroup is of the form $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Then, this is in fact a 2-dimensional vector space over $\mathbb{Z}/5\mathbb{Z}$, meaning that

$$\operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}),$$

which has order 480. In particular, there is some nontrivial automorphism from $\mathbb{Z}/3\mathbb{Z} \rightarrow \operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$, which we can find by selecting an element of order 3 from $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$, which emerges from the fact that $480 = 2^5 \cdot 3 \cdot 5$ admits a 3-Sylow subgroup. This gives the nonabelian group $(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes_f \mathbb{Z}/3\mathbb{Z}$.

(b) We observe that there are two abelian groups of order 75, given by

$$\begin{aligned}G_1 &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\\ G_2 &= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}.\end{aligned}$$

The reason G_1 and G_2 are not isomorphic is that there are no elements of order 25 in G_1, while (for example), $(0, 3)$ has order 5^2 in G_2.

In order to show that any two non-abelian groups of order 75 are isomorphic to each other, we start by showing that any non-abelian group of order 75 is of the form above. Since there is one 5-Sylow subgroup, we observe that said 5-Sylow subgroup is a group of order p^2, meaning that it has two forms. Either it is $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/25\mathbb{Z}$ by the classification of finite abelian groups. In the former case, we showed that $\mathbb{Z}/3\mathbb{Z}$ admits a nontrivial automorphism to $\operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$.

On the other hand, we observe that $\operatorname{aut}(\mathbb{Z}/25\mathbb{Z}) = (\mathbb{Z}/25\mathbb{Z})^{\times}$, which has 20 elements. Yet, this means there is no nontrivial homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to $(\mathbb{Z}/25\mathbb{Z})^{\times}$ by Lagrange's Theorem. Therefore we only need to consider homomorphisms from $\mathbb{Z}/3\mathbb{Z} \to \operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$.

Now, suppose we have two nontrivial homomorphisms $f_1 \colon \mathbb{Z}/3\mathbb{Z} \to \operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ and $f_2 \colon \mathbb{Z}/3\mathbb{Z} \to \operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$. Since these homomorphisms are nontrivial, they are injective (by Lagrange's Theorem), so $P_1 := \operatorname{im}(f_1)$ and $P_2 := \operatorname{im}(f_2)$ are 3-Sylow subgroups. Let $m_1 = f_1(1)$ and $m_2 = f_2(1)$ be generators for P_1 and P_2 respectively. Then, there is some $g \in \operatorname{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ such that for all $\ell \in \mathbb{Z}/3\mathbb{Z}$, we have $gf_1(\ell)g^{-1} = f_2(\ell)$. In particular, since the automorphisms f_1 and f_2 are conjugate, it follows from the result in Problem 2 that these two semidirect products are isomorphic.

Thus, there are exactly three groups of order 75 up to isomorphism.

Problem (Problem 4)**:** Let G be a group of order $n = 2k$, where k is odd. Show that G is not simple. You can use the following steps.

(a) Consider the injection $\rho \colon G \hookrightarrow S_n$ given by Cayley's Theorem. Let $H = \langle x \rangle$ be a subgroup of G of order 2. Show that $\rho(x)$ is an odd permutation. Deduce that $\operatorname{im}(\rho) \cap A_n$ is a normal subgroup of $\operatorname{im}(\rho)$ of index 2.

(b) Show that G has a subgroup of index 2.

Solution: Let $\rho \colon G \hookrightarrow S_n$ be the permutation representation for the left-regular action given by Cayley's theorem. If $H = \langle x \rangle$ is a subgroup of order 2, then x has order 2. Since injective homomorphisms preserve order, it follows that $\rho(x)$ has order 2.
Decomposing $\rho(x)$ into disjoint cycles,

$$\rho(x) = \tau_1 \cdots \tau_r,$$

we observe that each of the τ_i are transpositions since $\rho(x)$ has order 2. Furthermore, since the action of G on itself is free, it follows that we cannot have any identity permutations in the cycle decomposition of $\rho(x)$ (as x is not identity), meaning that there are k such transpositions. Since k is odd, $\rho(x)$ is thus an odd permutation.

In particular, since identity is an even permutation and $\rho(x)$ is an odd permutation, it follows that the composition $\operatorname{sgn} \circ \rho \colon G \to \{-1, 1\}$ is a surjective group homomorphism, so the kernel of this map is a proper normal subgroup of G. Thus, G is not simple.

Problem (Problem 5)**:** Classify all groups up of order 28.

Solution: We start by analyzing the nature of the Sylow subgroups. Writing $28 = 2^2 \cdot 7$, we observe that there is at least one 7-Sylow subgroup and at least one 2-Sylow subgroup. Yet, if there were more than one 7-Sylow subgroup, then there would have to be at least 8, but $8 \nmid 4$. Thus, there is a unique 7-Sylow subgroup. Similarly, since the number of 2-Sylow subgroups is odd and divides 7, it follows that there must be a unique 2-Sylow subgroup. This subgroup is also normal.

Thus, right away, we are able to use the classification of finite abelian groups to find two such groups of order 28, given by

$$\begin{aligned} G_1 &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ G_2 &= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}. \end{aligned}$$

These groups are not isomorphic to each other since G_1 contains an element of order 4 and G_2 does not.

Next, we consider all homomorphisms from $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ respectively into $(\mathbb{Z}/7\mathbb{Z})^{\times}$. Observe that $(\mathbb{Z}/7\mathbb{Z})^{\times} \cong \mathbb{Z}/6\mathbb{Z}$. There is thus an element of order 2 in $(\mathbb{Z}/7\mathbb{Z})^{\times}$, namely the equivalence class $[6]$, so we define homomorphisms $\varphi\colon \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^{\times}$ and $\psi\colon \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^{\times}$ by taking $1 \mapsto [6]$ and $(0,1) \mapsto [6], (1,0) \mapsto [1]$ respectively. The corresponding semidirect products $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ are not isomorphic to each other since the former contains the element $(0,1)$ that has order 4, while the latter does not contain any element of order 4.

The only case we need to verify is for the semidirect product $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, since we may also define $(1,0) \mapsto [6], (0,1) \mapsto [1]$ as another map from $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^{\times}$. Yet, these are isomorphic under the map

$$\begin{gathered}\Psi\colon \mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_1} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_2} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \\ (x,(y,z)) \mapsto (x,(z,y)).\end{gathered}$$

Thus, the four isomorphism classes for groups of order 28 are given by the following:

- $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/7\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/7\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.