

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 ζ_1, \dots, ζ_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 $\varphi_1, \varphi_2: G \rightarrow \text{aut}(H)$ be homomorphisms such that $\text{im}(\varphi_1)$ and $\text{im}(\varphi_2)$ 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 case that G is an infinite cyclic group, operating under the assumption that φ_1 and φ_2 are injective. 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 $g \in \text{aut}(H)$ such that $gM_1g^{-1} = M_2$. Conjugation is an isomorphism, so this means that $g\varphi_1(x)g^{-1} = \varphi_2(x)$ as generators are mapped to generators under isomorphism.

Define the map $\psi: H \rtimes_{\varphi_1} G \rightarrow H \rtimes_{\varphi_2} G$ 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:

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

Therefore, we only need to show the case for when G is of finite order.

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^2q , 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

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

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

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

$$G_1 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$G_2 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}.$$

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 $\text{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$. On the other hand, we observe that $\text{aut}(\mathbb{Z}/25\mathbb{Z}) = (\mathbb{Z}/25\mathbb{Z})^\times$, 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 $\mathbb{Z}/3\mathbb{Z} \rightarrow \text{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$.

Now, suppose we have two nontrivial homomorphisms $f_1: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ and $f_2: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$. Since these homomorphisms are nontrivial, they are injective (by Lagrange's Theorem), so $P_1 := \text{im}(f_1)$ and $P_2 := \text{im}(f_2)$ 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 $g \in \text{aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ 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.