Hints and solutions to Problems 3

1) Let $m = |G|$ and $n = |H|$. Then $|G \times H| = m \cdot n$.

   We show first that if G and H satisfy (a) and (b) then $G \times H$ is cyclic. Denote g and h generators of G and H, respectively. We claim that (g, h) generates $G \times H$. In fact, let l be the order of (g, h). Then $(e_G, e_H) = (g, h)^l = (g^l, h^l)$, and so $g^l = e_G$ and $h^l = e_H$. By part (ii) of the corollary after Definition 2.13 in the Lecture Notes we have then that m and n divide l. Since $\gcd(m, n) = 1$ we know that the lowest common multiple of m and n is their product $m \cdot n$. We conclude that $m \cdot n$ divides l. However the order of (g, h) can be at most $m \cdot n = |G \times H|$ and so we have $\mathrm{ord}(g, h) = mn$, *i.e.* (g, h) is a generator of $G \times H$ and the product group is cyclic.

   For the other direction. Let (g, h) be a generator of $G \times H$. We have homomorphisms of groups $\pi_G : G \longrightarrow G \times H$, $x \mapsto (x, e_H)$ and $\pi_H : H \longrightarrow G \times H$, $y \mapsto (e_G, y)$, which are one-to-one and so G and H are isomorphic to subgroups of the cyclic group $G \times H$. Since subgroups of cyclic groups are cyclic by Lemma 2.4 (iv) of the Lecture Notes we get (a), *i.e.* both G and H are cyclic groups.

   We show that also (b) holds by contradiction. Assume that m and n are not coprime. Then the lowest common multiplier l of m and n is strictly smaller that $m \cdot n$. Since m and n divide l we have by part (i) of the corollary after Definition 2.13 of the Lecture Notes that as $g^m = e_G$ and $h^n = e_H$ also $g^l = e_G$ and $h^l = e_H$. Therefore $(g, h)^l = (e_G, e_H)$ and so the order of (g, h) is $l < m \cdot n = |G \times H|$, contradicting that (g, h) generates the product group $G \times H$.

2) Since H is abelian we have

$$\begin{aligned} \alpha(ghg^{-1}h^{-1}) &= \alpha(g) \cdot \alpha(h) \cdot \alpha(g)^{-1} \cdot \alpha(h)^{-1} \\ &= \alpha(g) \cdot \alpha(g)^{-1} \cdot \alpha(h) \cdot \alpha(h)^{-1} \\ &= e_H \,, \end{aligned}$$

   and so $[G, G] \subseteq \operatorname{Ker} \alpha$. Hence the claim follows from part (i) of the first isomorphism theorem.

3) Let g be a cycle of length 2 and h one of length 3 in S_3. By Lagrange's theorem the subgroup generated by g, h has at least 6 elements and so is equal S_3. Hence if $\alpha \in \mathrm{Aut}(S_3)$ then α is determined by the images $\alpha(g)$ and $\alpha(h)$. Since α is an automorphism these images have to be again of order 2 and 3, respectively. Hence there are 3 possibilities for $\alpha(g)$ and 2 possibilities for $\alpha(h)$, which means there can be at most $6 = 2 \cdot 3$ automorphisms of S_3.

   On the other hand the center of S_3 is trivial, see Example 2.16 of the Lecture Notes and so by Example 3.12 of the Lecture Notes we have $\mathrm{Inn}(S_3) \simeq S_3$, *i.e.* the subgroup $\mathrm{Inn}(S_3)$ of $\mathrm{Aut}(S_3)$ has 6 elements. Hence we get the claim $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$.

4) To verify this, let H, K be groups and $\alpha : K \longrightarrow \mathrm{Aut}(H)$ be a homomorphism of groups with associated semidirect product $H \rtimes_\alpha K$. Set

$$H_1 := \Big\{ (h, e_K) \,\Big|\, h \in H \Big\} \quad \text{and} \quad K_1 := \Big\{ (e_H, k) \,\Big|\, k \in K \Big\}.$$

Then it is straightforward to check that

$$H \longrightarrow H \rtimes_\alpha K\,,\ h \longmapsto (h, e_K)$$

and

$$K \longrightarrow H \rtimes_\alpha K\,,\ k \longmapsto (e_H, k)$$

are injective homomorphism of groups whose images are H_1 and K_1, respectively. Hence we have $H \simeq H_1$ and $K \simeq K_1$. We claim now that $G := H \rtimes_\alpha K$ is the internal semidirect product of H_1 and K_1.

Clearly the intersection $H_1 \cap K_1$ contains only (e_H, e_K), the neutral element of G, and since

$$(h, k) = (h, e_K) \cdot (e_H, k)$$

we have $H_1K_1 = G$ as well. Finally we have to show that H_1 is a normal subgroup. This follows from the following computation:

$$\begin{aligned}(h,k)\cdot(x,e_K)\cdot(h,k)^{-1} &= (h,k)\cdot(x,e_K)\cdot(\alpha(k^{-1})(h^{-1}),k^{-1}) \\ &= (h,k)\cdot\Big(x\cdot[\alpha(k^{-1})(h^{-1})]\,,\ k^{-1}) \\ &= \Big(h\cdot\alpha(k)\big(x\cdot[\alpha(k^{-1})(h^{-1})]\big)\,,\ e_K\Big) \ \in\ K_1\end{aligned}$$

for all $x, h \in H$ and $k \in K$.

5) If G is abelian then $(x \cdot y)^2 = x^2 \cdot y^2$, and so in this case $G \longrightarrow G$, $g \mapsto g^2$, is a homomorphism of groups. For the other direction, if this is a homomorphism of groups then

$$x \cdot (y \cdot x) \cdot y = (x \cdot y)^2 = x^2 \cdot y^2$$

for all $x, y \in G$. Multiplying this equation by x^{-1} on the left, and by y^{-1} on the right gives $y \cdot x = x \cdot y$, *i.e.* G is abelian.

To show that in case G is abelian of odd order this map is an isomorphism it is enough to show that it is injective (an injective map of a finite set into itself is automatically surjective). Assume that $x^2 = e$ for some $x \in G$. Let $|G| = 2m+1$ for some integer $m \geq 0$. Then we have by the corollary after Definition 2.13 in the Lecture notes $x^{2m+1} = e$, and so

$$e = x^{2m+1} = (x^2)^m \cdot x = e^m \cdot x = x\,.$$

Hence the kernel of $G \longrightarrow G$, $g \mapsto g^2$, contains only the neutral element, and so this map is one-to-one.

6) Let $h \in H$. We have to show that then $x \cdot h \cdot x^{-1} \in H$ for all $x \in G$. Since H contains the commutator subgroup we have $x \cdot h \cdot x^{-1} \cdot h^{-1} \in H$ for all $x \in G$, and so also

$$x \cdot h \cdot x^{-1} = (x \cdot h \cdot x^{-1} \cdot h^{-1}) \cdot h \ \in\ H$$

for all $x \in G$.

That the quotient group G/H is then normal follows since $x{\cdot}y{\cdot}x^{-1}{\cdot}y^{-1} \in [G,G] \subseteq H$ implies $(x \cdot y) \cdot (y \cdot x)^{-1} \in H$, and so $(xy)H = (yx)H$, which in turn gives

$$xH \cdot yH \;=\; yH \cdot xH$$

for all $x, y \in G$. Hence G/H is commutative.

7) Let $\alpha : G_1 \xrightarrow{\simeq} G_2$ be an isomorphism of groups. Then

$$\mathrm{Aut}(G_2) \;\longrightarrow\; \mathrm{Aut}(G_1)\,,\;\rho \longmapsto \alpha^{-1} \circ \rho \circ \alpha$$

is an isomorphism of groups as is straightforward to check.

The cyclic groups $\mathbb{Z}/8$ and $\mathbb{Z}/12$ are not isomorphic, but there automorphism groups are both isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. In fact, by Example 3.14 in the Lecture Notes we know that $\mathrm{Aut}(\mathbb{Z}/8) \simeq (\mathbb{Z}/8)^\times$ and $\mathrm{Aut}(\mathbb{Z}/12) \simeq (\mathbb{Z}/12)^\times$. We have $|(\mathbb{Z}/8)^\times| = |(\mathbb{Z}/12)^\times| = 4$ and in both groups all elements have order 2, which implies that

$$(\mathbb{Z}/8)^\times \;\simeq\; (\mathbb{Z}/12)^\times \;\simeq\; \mathbb{Z}/2 \times \mathbb{Z}/2$$

by Problems 2, 4).