Solutions #3

1. Let $H$ and $K$ be two subgroups of a group $G$. A double coset is a subset of $G$ of the form

$$HgK := \{hggk | h \in H, k \in K\}.$$ 

(a) Prove that the double cosets of $G$ partition $G$, i.e., that any two double cosets $Hg'K$ and $Hg''K$ either do not intersect or coincide.

(b) Is it true that the double cosets have the same size?

Solution. (a) If $g \in Hg'K$, then $g = h'g'k'$ for some $h' \in H$ and $k' \in K$. Thus $HgK = H(h'g'k')K = (Hh')g'(k'K) = HgK$ (Justify!). Assume now that the double cosets $Hg'K$ and $Hg''K$ intersect and $g$ is a common element. Then we have $HgK = Hg'K$ and $HgK = Hg''K$, proving that $Hg'K = Hg''K$.

(b) No. Let $G = S_3$ and $H = K = \{e, (12)\}$. Then there are two double cosets: $HeK = H$ and $H(23)K = S_3 \setminus H$ which are of different size. (Verify!)

2. (a) Let $C = (123 \ldots n) \in S_n$. Determine the type of the cycle decomposition of $C^k$ for $1 \leq k \leq n$, i.e., how many cycles (and of what lengths) appear in the cycle decomposition of $C^k$.

(b) Let $\sigma = C_1C_2 \ldots C_k$ be the decomposition of $\sigma$ into disjoint cycles of lengths $l_1, l_2, \ldots, l_k$ respectively. What is the order of $\sigma$?

(c) What are the possible orders of elements of $S_{10}$?

Solution. (a) Since $C^m(i) \equiv i + s \pmod{n}$, we see that $(C^k)^s(i) = i$ if and only if $n$ divides $ks$. Thus $i$ belongs to an $s$-cycle of $C^k$ if $s$ is the smallest integer such that $n$ divides $ks$. In other words, $i$ belongs to a cycle of length $n' := n/d$, where $d$ is the GCD of $n$ and $k$. Since this is independent of $i$, we conclude that $C^k$ is a product of $d$ disjoint cycles of length $n'$ each.

(b) Since the cycles $C_1, C_2, \ldots, C_k$ commute pairwise and their orders are respectively $l_1, l_2, \ldots, l_k$, the order of $\sigma$ is the least common multiple of $l_1, l_2, \ldots, l_k$.

(c) The possible orders of elements of $S_{10}$ are the least common multiples of partitions $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ of $10$. To find all possible orders, one can go through all partitions (a total of 42) of 10 and find the corresponding orders. Alternatively, for a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ of 10 with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 1$, let $\ell(\lambda)$ denote the LCM of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$. Note that $\ell(\lambda) = \text{LCM}(\lambda_1, \ell(\lambda'))$, where $\lambda' = (\lambda_2, \ldots, \lambda_k)$. For $\lambda_1 \geq 5$, the partition $\lambda'$ runs over all partitions of $10 - \lambda_1$; for $\lambda \leq 4$, $\lambda'$ runs over partitions of $10 - \lambda_1$ whose first part is no greater than $\lambda_1$. The list below gives us the possible orders for partitions with $\lambda_1 \geq 5$:

<table>
<thead>
<tr>
<th>$\lambda_1$</th>
<th>possible orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>21, 14, 7</td>
</tr>
<tr>
<td>6</td>
<td>12, 6</td>
</tr>
<tr>
<td>5</td>
<td>30, 20, 15, 10, 5</td>
</tr>
</tbody>
</table>
To verify the table above, say $\lambda_1 = 5$. Then we consider partitions $\lambda'$ of 5. These may have $\ell(\lambda') = 5, 4, 6, 3, 2, 1$. Taking $\text{LCM}(\lambda_1, \ell(\lambda'))$ we get the possible values 30, 20, 15, 10, 5 for $\ell(\lambda)$.
One checks easily that if $\lambda_1 = 4$ then the possible values of $\ell(\lambda)$ are 12, 4; if $\lambda_1 = 3$ then the possible values of $\ell(\lambda)$ are 6, 3; if $\lambda_1 = 2$ then $\ell(\lambda) = 2$; and if $\lambda_1 = 1$ then $\ell(\lambda) = 1$.
This leads us to the final answer for the possible values of $\ell(\lambda)$ in increasing order:

\[30, 21, 20, 15, 12, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1.\]

3. Let $Z(G)$ denote the centre of $G$. Assume that $G/Z(G)$ is cyclic. Prove that $G$ is abelian.

**Solution.** Assume $G/Z(G) = \langle x \rangle$ and let $x \in G$ be such that $x = xZ(G)$. If $g \in G$, then $gZ(G) = x^i$ for some $i$ and hence $gZ(G) = x^iZ(G)$. In other words, $x^{-i}g = z \in Z(G)$ or, any element $g \in G$ can be written as $g = x^i z$ for some $i \in \mathbb{Z}$ and $z \in Z(G)$.
Let $g_1 = x^i z_1, g_2 = x^j z_2 \in G$. Then

\[g_1 g_2 = (x^i z_1)(x^j z_2) = x^i x^j z_1 z_2 = x^{i+j} z_1 z_2 = (x^i z_2)(x^j z_1) = g_2 g_1.\]
Note that $Q_8$ is an example of a non-abelian group for which $G/Z(G)$ is abelian. Indeed, $Z(Q_8) = \langle -1 \rangle$ and $Q_8/Z(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian.

4. Let $[G, G] := \langle xyx^{-1}y^{-1} | x, y \in G \rangle$ be the commutator subgroup of $G$. Prove that
(a) $[G, G]$ is normal in $G$ and $G/[G, G]$ is abelian;
(b) a subgroup $H$ of $G$ contains $[G, G]$ if and only if $H$ is normal and $G/H$ is abelian.

**Solution.** (a) Let $S \subset G$ be a subset of $G$ and let $N = \langle S \rangle$ be the subgroup of $G$ generated by $S$. To prove that $N$ is a normal subgroup of $G$ it suffices to show that, for every $g \in G$ and $s \in S$, we have $gsg^{-1} \in N$ (why?). So, if $s = xyx^{-1}y^{-1}$, we have

\[gsg^{-1} = gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1}x^{-1})(xyx^{-1}y^{-1}g^{-1}) = (gxg^{-1}x^{-1})(x(gy)x^{-1}(gy))^{-1};\]
proving that $[G, G]$ is normal.

For $x, y \in G$ the fact that $x^{-1}y^{-1}xy \in [G, G]$ implies


(b) If $H$ contains $[G, G]$, then the Fourth Isomorphism theorem implies that $H$ is normal in $G$ if and only if $H/[G, G]$ is a normal subgroup of $G/[G, G]$. Since $G/[G, G]$ is abelian, $H/[G, G]$ is normal and abelian, completing this direction.

Conversely, let $H$ be normal and assume $G/H$ is abelian. For any $x, y \in G$, we have $xyH = yxH$ in $G/H$ which implies that $x^{-1}y^{-1}xy \in H$ and hence $[G, G] \leq H$.

5. Let $G_1$ and $G_2$ be finite groups whose orders are coprime. Prove that

\[\text{Aut}(G_1 \times G_2) \cong \text{Aut} G_1 \times \text{Aut} G_2.\]
Solution. As a first step we show how homomorphisms \( G_1 \times G_2 \to G_1 \times G_2 \) are related to pairs of homomorphisms \( G_1 \to G_1 \) and \( G_2 \to G_2 \).

For \( j = 1, 2 \), let \( \iota_j : G_j \to G_1 \times G_2 \) and \( \pi_j : G_1 \times G_2 \to G_j \) denote the corresponding canonical injection and surjection respectively. Given a homomorphism \( \theta : G_1 \times G_2 \to G_1 \times G_2 \), define the homomorphisms

\[
\begin{align*}
\theta_1 & := \pi_1 \circ \theta \circ \iota_1 : G_1 \to G_1 \\
\theta_2 & := \pi_2 \circ \theta \circ \iota_2 : G_2 \to G_2 \\
\phi & := \pi_2 \circ \theta \circ \iota_1 : G_1 \to G_2 \\
\psi & := \pi_1 \circ \theta \circ \iota_2 : G_2 \to G_1.
\end{align*}
\]

Consider \( \text{Im} \phi \). On one hand, \( \text{Im} \phi < G_2 \) and hence \( |\text{Im} \phi| \) divides \( |G_2| \). On the other hand, \( \text{Im} \phi \cong G_1 / \ker \phi \) implies that \( |\text{Im} \phi| \) divides \( |G_1| \). Since \( |G_1| \) and \( |G_2| \) are coprime we conclude that \( |\text{Im} \phi| = 1 \), i.e., that \( \phi \) is the trivial homomorphism. Similarly, \( \psi \) is trivial. Next we calculate

\[
\theta(g_1, e) = (\theta \circ \iota_1)(g_1) = ((\pi_1 \circ \theta \circ \iota_1)(g_1), (\pi_2 \circ \theta \circ \iota_1)(g_1)) = (\theta_1(g_1), e)
\]

and, similarly, \( \theta(e, g_2) = (e, \theta_2(g_2)) \). Combining these we obtain

\[
\theta(g_1, g_2) = \theta((g_1, e)(e, g_2)) = \theta(g_1, e)\theta(e, g_2) = (\theta_1(g_1), \theta_2(g_2)).
\]

Conversely, given homomorphisms \( \theta_1 : G_1 \to G_1 \) and \( \theta_2 : G_2 \times G_2 \), the formula

\[
\theta(g_1, g_2) := (\theta_1(g_1), \theta_2(g_2))
\]

defines a homomorphism \( \theta : G_1 \times G_2 \to G_1 \times G_2 \).

The constructions above establish a bijection

\[
\text{Hom}(G_1 \times G_2, G_1 \times G_2) \leftrightarrow \text{Hom}(G_1, G_1) \times \text{Hom}(G_2, G_2)
\]

where \( \text{Hom}(G, H) \) denotes the set of homomorphisms from \( G \) to \( H \). Moreover, this bijection respects composition of homomorphisms. Verify!

The equation \( \ker \theta = \ker \theta_1 \times \ker \theta_2 \) shows that \( \theta \) is an automorphism if and only if both \( \theta_1 \) and \( \theta_2 \) are automorphisms. In other words, we have a bijection

\[
\text{Aut}(G_1 \times G_2) \leftrightarrow \text{Aut} G_1 \times \text{Aut} G_2
\]

which respects compositions, i.e., is a homomorphism of groups. This completes the proof that \( \text{Aut}(G_1 \times G_2) \cong \text{Aut} G_1 \times \text{Aut} G_2 \). \( \square \)