Solutions #5

1. Let $G < S_n$ be a group of order $p^k$ where $p$ is a prime number which is coprime with $n$. Prove that there is $1 \leq i \leq n$ such that $\sigma(i) = i$ for every $\sigma \in G$.

Solution. Let $X := \{1, 2, \ldots, n\}$. Then $G$ acts on $X$ and $n = |X|$ is the sum of the cardinalities of the orbits of $G$ in $X$. Since $n$ and $p$ are coprime, there is an orbit $O_i$ whose cardinality $|O_i|$ is not divisible by $p$. On the other hand, $|O_i| = [G : G_i]$ is a divisor of $|G| = p^k$. This implies that $|O_i| = [G : G_i] = 1$ and hence $G_x = G$, i.e., $\sigma(i) = i$ for every $\sigma \in G$. □

2. Assume that $G$ acts on $X$ and define $X^g := \{ x \in X | g \cdot x = x \}$.

(a) Prove that the number of orbits of $G$ on $X$ equals $\frac{1}{|G|} \sum_{g \in G} |X^g|$.

(b) If $|X| > 1$ and $G$ acts transitively on $X$, prove that there exists $g \in G$ such that $g \cdot x \neq x$ for every $x \in X$.

Solution. (a) Let $O_1, O_2, \ldots, O_k$ be the orbits of $G$ in $X$ and let

$$Y := \{(g, x) \in G \times X | g \cdot x = x\} \subset G \times X.$$ 

We have

$$Y = \bigsqcup_{g \in G} X^g$$

and

$$Y = \bigsqcup_{x \in X} G_x = \bigsqcup_{i=1}^k (\bigsqcup_{x \in O_i} G_x).$$

Note that

$$|\bigsqcup_{x \in O_i} G_x| = \sum_{x \in O_i} |G_x| = \sum_{x \in O_i} \frac{|G|}{|O_i|} = \frac{|G|}{|O_i|} \sum_{x \in O_i} 1 = \frac{|G|}{|O_i|} |O_i| = |G|.$$ 

Using the two decompositions of $Y$ above we have

$$|Y| = \sum_{g \in G} |X^g| = \sum_{i=1}^k |G| = k|G|,$$

which proves that the number of orbits, $k$, equals $\frac{1}{|G|} \sum_{g \in G} |X^g|$.

(b) $G$ acting transitively on $X$ means that $X$ is a single orbit. Applying (a) we get $|G| = \sum_{g \in G} |X^g|$. Since $|X^g| = |X| > 1$ and $|X^g| \geq 0$, we conclude that $|X^g| = 0$ for some $g \in G$. This implies that $g \cdot x \neq x$ for every $x \in X$. □

3. Let $N$ be a normal subgroup of $G$ and let $P$ be a Sylow $p$-subgroup of $G$. Show that $P \cap N$ and $PN/N$ are Sylow $p$-subgroups of $N$ and $G/N$ respectively.

Solution 1. Let $Q$ be a Sylow $p$-subgroup of $N$. Then $Q$ is a $p$-subgroup of $G$ and hence there is $g \in G$ such that $Q \subset gPg^{-1}$. Also $Q \subset N = gNg^{-1}$ implies that $Q \subset gP^g^{-1} \cap gNg^{-1} = g(P \cap N)g^{-1}$. In particular, $|Q| \leq |P \cap N|$. Since $P \cap N$ is a $p$-subgroup of $G$ (and hence of $N$), the last inequality shows that $P \cap N$ is a Sylow $p$-subgroup of $N$.
Let $|G| = p^m n, |N| = p^n l$. Then $|G/N| = p^{\alpha - \beta} s$ where $s = \frac{n}{l}$ and $|P \cap N| = p^\beta$ from above. Furthermore, $PN/N \cong P/P \cap N$ implies that $|PN/N| = |P/P \cap N| = p^{\alpha - \beta}$ proving that $PN/N$ is a Sylow $p$-subgroup of $G/N$. □

Solution 2. Let, as above, $|G| = p^m n, |N| = p^n l$, and $|G/N| = p^{\alpha - \beta} s$. The observation $m = [G : P] = [G : PN][PN : N]$ implies that $[G : PN] = t$ is not divisible by $p$ and the fourth isomorphism theorem implies that $[G/N : PN/N] = [G : PN]$. Combining the two we conclude that $|PN/N| = p^{\alpha - \beta} t$ for some divisor $t$ of $m$. On the other hand, $PN/N \cong P/P \cap N$ implies that $PN/N$ is a $p$-group, so we conclude that $|PN/N| = p^{\alpha - \beta}$, i.e., that $PN/N$ is a Sylow $p$-subgroup of $G/N$. Now the isomorphism $PN/N \cong P/P \cap N$ implies that $|P \cap N| = p^\beta$, i.e., $P \cap N$ is a Sylow $p$-subgroup of $N$. □

4. Prove that there are no simple groups of orders 80, 90, or 1000.

Solution. $|G| = 80$, first argument. Assume $|G| = 80 = 2^4 \times 5$ and $G$ is simple. Then $n_5$ divides 16 and $n_5 \equiv 1 \pmod{5}$; the options are $n_5 = 1$ or $n_5 = 16$. Since $G$ is simple $n_5 \neq 1$, i.e., $n_5 = 16$. Any two Sylow 5-subgroups intersect trivially and every Sylow 5-subgroup contains 4 elements of order 5. Conversely, every element of $G$ of order 5 is contained in a Sylow 5-subgroup. Hence $G$ contains $16 \times 4 = 64$ elements of order 5 and 16 elements of order different from 5. Since the elements of any Sylow 2-subgroup of $G$ are of orders dividing 16, there is room only for one Sylow 2-subgroup which implies that $G$ is not simple.

$|G| = 80$, second argument. Assume $|G| = 80 = 2^4 \times 5$ and $G$ is simple. Then $n_2$ divides 5 and $n_2 \equiv 1 \pmod{2}$; the options are $n_2 = 1$ or $n_2 = 5$. Since $G$ is simple $n_2 \neq 1$, i.e., $n_2 = 5$. The group $G$ acts transitively on the set $\text{Syl}_2(G)$ by conjugation, giving rise to a homomorphism of groups $\varrho : G \to S_5$. Since $|\text{Im}\varrho|$ divides both $|G| = 80$ and $|S_5| = 5$, we conclude that $|\text{Im}\varrho| \neq 80$ and hence $|\text{Ker}\varrho| \neq 1$. In other words, $\text{Ker}\varrho$ is a normal subgroup of $G$ which neither $\{e\}$ nor $G$, i.e., $G$ is not simple.

$|G| = 90$. Assume $|G| = 90 = 2 \times 3^2 \times 5$ and $G$ is simple. Then $n_5 = 6$ and the action of $G$ on $\text{Syl}_5(G)$ gives rise to a homomorphism $\varrho : G \to S_6$. Since $G$ is simple, $\varrho$ is an injection, i.e., $G$ is isomorphic to a subgroup of $S_6$. If $P$ is a Sylow 5-subgroup of $G$ then $|G : N_G(P)| = n_5 = 6$, i.e., $|N_G(P)| = 15$. The classification of groups of order $pq$ implies that $N_G(P) \cong \mathbb{Z}_{15}$. Thus $N_G(P)$ (and hence, $G$) contains an element of order 15. On the other hand, $S_6$ does not contain elements of order 15 which contradicts the conclusion above that $G$ is isomorphic to a subgroup of $S_6$.

$|G| = 1000$. If $|G| = 1000 = 2^3 \times 5^3$ then $n_5$ divides 8 and $n_5 \equiv 1 \pmod{5}$ implies that $n_5 = 1$. Thus $G$ is not simple. □

5. Prove that the free product $\mathbb{Z}_2 \ast \mathbb{Z}_2$ is isomorphic to the infinite dihedral group $D_\infty$. 


**Solution.** Let $H = \langle a \rangle \cong \mathbb{Z}_2$ and $K = \langle b \rangle \cong \mathbb{Z}_2$. Note that $a^2 = b^2 = e$ and $a^{-1} = a, b^{-1} = b$. Hence

$$H * K = \{abab \ldots aba, abab \ldots ab, bab \ldots aba, bab \ldots ab\}.$$  

Recall that $D_\infty = \langle r, s \mid s^2 = e, srs = r^{-1} \rangle = \{r^n, sr^n \mid n \in \mathbb{Z}\}$. Define the map $\varphi : D_\infty \to H * K$ by setting

$$\varphi(r^n) = \begin{cases} 
ab \ldots ab & \text{if } n \geq 0 \\
 \text{times ba} \ldots ba & \text{if } n < 0, \\
\text{times} -n & 
\end{cases}$$

$$\varphi(sr^n) = \begin{cases} 
ab \ldots ab & \text{if } n > 0 \\
 \text{times ba} \ldots ba & \text{if } n \leq 0, \\
\text{times} -n & 
\end{cases}$$

where, as usual, the empty word represents the element $e$. It is obvious by the explicit definition that $\varphi$ is a bijection. It is a tedious verification that $\varphi$ is a homomorphism. This completes the proof that $\mathbb{Z}_2 * \mathbb{Z}_2 \cong H * K \cong D_\infty$.

**Remark.** The idea for the proof above is that the elements $x = a, y = ab$ of $H * K$ satisfy the relations $x^2 = e, xyx = y^{-1}$. It also seems obvious that these relations determine $H * K$, i.e., that

$$H * K = \langle x, y \mid x^2 = e, xyx = y^{-1} \rangle.$$  

However, proving that certain relations in a group determine the group is usually difficult to prove. (Strictly speaking, the equations

$$D_\infty = \langle r, s \mid s^2 = e, srs = r^{-1} \rangle = \{r^n, sr^n \mid n \in \mathbb{Z}\}.$$  

also need justification.) For this reason, I provided above a more direct (and uglier) approach. \qed