More on Symmetric Groups and Direct Products

Ex: Find $|((1,2,3),(1,2))|$ in $S_3 \times S_2$.

Solution. $|(1,2,3)| = 3$ in S_3 and $|(1,2)| = 2$ in S_2, so $|((1,2,3),(1,2))| = \operatorname{lcm}(3,2) = 6$ in $S_3 \times S_2$.

This should feel very similar to our statement about the order of a product of disjoint cycles in S_n. Namely, the order of a product of disjoint cycles is the product of the lengths of the cycles. Considering the previous example, we see that $|((1,2,3),(1,2))|$ in $S_3 \times S_2$ is the same as $|(1,2,3)(4,5)|$ in S_5. This isn't an accident.

Thm: Given $m, n \in \mathbb{Z}^+$, $S_m \times S_n$ is isomorphic to a proper subgroup of S_{m+n}.

Proof. Let $m, n \in \mathbb{Z}^+$ and for each pair $(\sigma, \tau) \in S_m \times S_n$, define $\rho_{\sigma,\tau} : \{1, 2, \ldots, m+n\} \to \{1, 2, \ldots, m+n\}$ by

$$\rho_{\sigma,\tau}(k) = \begin{cases} \sigma(k) & \text{if } k \leq m \\ \tau(k-m) + m & \text{if } k > m \end{cases}$$

for $k = 1, 2, \ldots, m+n$. It is easily seen that $\rho_{\sigma^{-1},\tau^{-1}} \circ \rho_{\sigma,\tau} = \iota = \rho_{\sigma,\tau} \circ \rho_{\sigma^{-1},\tau^{-1}}$, so that $\rho_{\sigma^{-1},\tau^{-1}}$ is an inverse function for $\rho_{\sigma,\tau}$. This shows that $\rho_{\sigma,\tau} \in S_{m+n}$, so we henceforth suppress $\circ$.

Define $\phi : S_m \times S_n \to S_{m+n}$ by $\phi(\sigma, \tau) = \rho_{\sigma,\tau}$. We claim that ϕ is an injective map satisfying the homomorphism property. Indeed, if $\phi(\sigma_1, \tau_1) = \phi(\sigma_2, \tau_2)$, then $\rho_{\sigma_1,\tau_1} = \rho_{\sigma_2,\tau_2}$. But this implies $\sigma_1(k) = \sigma_2(k)$ for $k = 1, 2, \ldots, m$ and $\tau_1(k-m) + m = \tau_2(k-m) + m$ for $k = m+1, m+2, \ldots, m+n$. It is easily seen that these yield $\sigma_1 = \sigma_2$ and $\tau_1 = \tau_2$ and so $(\sigma_1, \tau_1) = (\sigma_2, \tau_2)$. Therefore ϕ is injective. To see that ϕ satisfies the homomorphism property, consider $(\sigma_1, \tau_1), (\sigma_2, \tau_2) \in S_m \times S_n$. Then $\phi((\sigma_1, \tau_1)(\sigma_2, \tau_2)) = \phi(\sigma_1\sigma_2, \tau_1\tau_2) = \rho_{\sigma_1\sigma_2,\tau_1\tau_2}$ and $\phi(\sigma_1, \tau_1)\phi(\sigma_2, \tau_2) = \rho_{\sigma_1,\tau_1}\rho_{\sigma_2,\tau_2}$. Now, for $1 \leq k \leq m$, we have $1 \leq \sigma_2(k) \leq m$ and so

$$\rho_{\sigma_1\sigma_2,\tau_1\tau_2}(k) = \sigma_1\sigma_2(k) = \rho_{\sigma_1,\tau_1}(\sigma_2(k)) = \rho_{\sigma_1,\tau_1}\rho_{\sigma_2,\tau_2}(k).$$

Similarly, if $m+1 \leq k \leq m+n$, then $m+1 \leq \tau_2(k-m) + m \leq m+n$ and so

$$\rho_{\sigma_1\sigma_2,\tau_1\tau_2}(k) = \tau_1\tau_2(k-m) + m = \rho_{\sigma_1,\tau_1}(\tau_2(k-m) + m) = \rho_{\sigma_1,\tau_1}\rho_{\sigma_2,\tau_2}(k).$$

We have shown that $\rho_{\sigma_1\sigma_2,\tau_1\tau_2} = \rho_{\sigma_1,\tau_1}\rho_{\sigma_2,\tau_2}$ and therefore ϕ satisfies the homomorphism property.

We proved in class that the image of any injective map between groups which satisfies the homomorphism property is a subgroup of the codomain, isomorphic to the domain. Therefore $\phi[S_m \times S_n]$ is a subgroup of S_{m+n}, isomorphic to $S_m \times S_n$.

To see that $\phi[S_m \times S_n]$ is proper, consider the transposition $(m, m+1) \in S_{m+n}$. We claim that $(m, m+1) \notin \phi[S_m \times S_n]$. That is, there is no $(\sigma, \tau) \in S_m \times S_n$ such that $\rho_{\sigma,\tau} = \phi(\sigma, \tau) = (m, m+1)$. To verify, note that, given $(\sigma, \tau) \in S_m \times S_n$, we have

$$\rho_{\sigma,\tau}(m) = \sigma(m) \leq m < m+1.$$

Therefore $\rho_{\sigma,\tau} \neq (m, m+1)$ and we conclude that $(m, m+1) \notin \phi[S_m \times S_n]$. Therefore, $\phi[S_m \times S_n]$ is a proper subgroup of S_{m+n}. □

We can upgrade the preceding theorem to more than one factor:

Thm: Given $m_i \in \mathbb{Z}^+$ for $i = 1, \ldots, k$, $S_{m_1} \times \cdots \times S_{m_k}$ is isomorphic to a proper subgroup of $S_{m_1+\cdots+m_k}$.

However, this theorem doesn't really capture the whole story. Not every permutation can be written as a product of disjoint cycles with each cycle corresponding to consecutive integers. Consider the following example.

Ex: $(1,2,3)(5,9,4)(6,8,7)$ is a permutation of $\{1,2,3,4,5,6,7,8,9\}$ and there is no set of numbers $m_1, m_2, \ldots, m_k$ such that $(1,2,3)(5,9,4)(6,8,7)$ is in the image of our ϕ from the above proof (of course generalized to the more general theorem above). Instead we should view each cycle as a permutation of its orbit. Namely,

$$(1,2,3) \in S_{\{1,2,3\}}, \quad (5,9,4) \in S_{\{4,5,9\}}, \quad (6,8,7) \in S_{\{6,7,8\}}.$$

We can show that $S_{\{1,2,3\}} \times S_{\{4,5,9\}} \times S_{\{6,7,8\}}$ is isomorphic to a subgroup of S_9 containing $(1,2,3)(5,9,4)(6,8,7)$.

To handle cases such as the example presents, see the fourth additional exercise on your homework for this week (Homework 5).