TheNumbersBook.com 2010

Dummit & Foote 1.3.10, 1.3.14

1.3.10 Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least positive residue mod m. Deduce that $|\sigma| = m$.

Note that applying σ onto an element, maps the element one index up. We prove by induction on the index:

(1) Base case: for $i = 1, \sigma^1(a_k) = a_{k+1 \mod m}$ which yields the index with least positive residue modulo m.

(2) Induction hypothesis: Suppose that $\sigma^n(a_k) = a_{(k+n) \mod m} = a_{k'}$ where k' is the least positive residue of $k+n$ modulo m.

(3) Consider $i = n+1$:

$$\begin{aligned}
\sigma^{n+1}(a_k) &= \sigma(\sigma^n(a_k)) \\
&= \sigma(a_{(k+n) \text{mod } m}) \\
&= \sigma(a_{k'}) \\
&= a_{k' \mod m} \\
&= a_{k''}
\end{aligned}$$

and we know that k'' is the least positive residue modulo m by the base case. By induction hypothesis, the result follows.

Consider the number of distinct values obtained by $k+i \mod m$: $0, 1, \cdots, m-1$. Thus, $|\sigma| = m$. ∎

1.3.14 Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

I first show the contrapositive of the forward direction: If its cycle decomposition is not a product of commuting p-cycles, then an element does not have order p in S_n:
Let $\sigma \in S_n$. Then, let $\sigma = c_1c_2\cdots c_n$ where c_i is a cycle and all cycles are disjoint. Note that by the contrapositive, there exists a c_i that has a different order than other cycles, say $|c_n| = k$. We now show that p is not the order of σ:

$$\sigma = c_1 c_2 \cdots c_n$$

$$\sigma^p = (c_1 c_2 \cdots c_n)(c_1 c_2 \cdots c_n) \cdots (c_1 c_2 \cdots c_n)$$

Since the cycles commute, we rearrange them without suffering the consequences,

$$\begin{aligned}
\sigma^p &= (c_1 c_2 \cdots c_n)(c_1 c_2 \cdots c_n) \cdots (c_1 c_2 \cdots c_n) \\
&= (c_1 c_1 \cdots c_1)(c_2 c_2 \cdots c_2) \cdots (c_n c_n \cdots c_n) \\
&= (c_1)^p (c_2)^p \cdots (c_n)^p
\end{aligned}$$

We immediately realize that $(c_n)^p$ will not give us the identity because k does not divide p (p is prime) and so the whole expression cannot equal e. This implies that $\sigma^p \neq e$. Therefore, $|\sigma| \neq p$.
We now prove the reverse direction:
If its cycle decomposition is a product of commuting p-cycles, then the order is p. Again, let $\sigma \in S_n$, and $\sigma = c_1 c_2 \cdots c_n$. Suppose $|\sigma| = k$,

$$\begin{aligned}
\sigma^k = (c_1 c_2 \cdots c_n)(c_1 c_2 \cdots c_n) \cdots (c_1 c_2 \cdots c_n) &= (c_1 c_1 \cdots c_1)(c_2 c_2 \cdots c_2) \cdots (c_n c_n \cdots c_n) \\
&= (c_1)^k (c_2)^k \cdots (c_n)^k
\end{aligned}$$

This last equality comes from rearranging the cycles. Recall from the first problem that if c_i is an m-cycle, then $|c_i| = m$. We know that each cycle is a p-cycle, so $|c_i| = p$. If we let $k = p$ in the above equation, then:

$$\begin{aligned}
(c_1)^p (c_2)^p \cdots (c_n)^p &= ee \cdots e \\
&= e
\end{aligned}$$

So, $\sigma^p \leq e$. Can $k < p$? If it did, then we would have $\sigma^k = (c_1)^k \cdots (c_n)^k$, but none of the cycles would be the identity because they are p-cycles, and so each cycle satisfies the equation $c_i^p = e$. This implies that $\sigma^k \neq e, k < p$. So, $k = p$ and $|\sigma| = p$.
We have now proven both directions. We are therefore confident in saying that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles.

$\blacksquare$