Algebraic Structures (MST20010)

Problem sheet 4

1. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 3 & 9 & 6 & 5 & 8 & 7 \end{pmatrix}.$

   (b) $(1\ 2\ 3\ 5\ 7)(2\ 4\ 7\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 7 & 3 & 6 & 8 & 9 \end{pmatrix}.$

2. We know that the order of σ is 4 since it is a cycle of length 4. Therefore $\sigma^4 = \mathrm{id}$, $\sigma^5 = \sigma$, $\sigma^6 = \sigma^2$, ...and in general, if $n = 4q + r$ with $r \in \{0, 1, 2, 3\}$ then $\sigma^n = \sigma^r$ (since $\sigma^n = \sigma^{4q}\sigma^r = (\sigma^4)^q\sigma^r = \mathrm{id}\,\sigma^r = \sigma^r$).

   So we only have to compute σ^2 and σ^3.

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}, \ \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}.$$

3. (a) We simply do the integer division of m by k and obtain: $m = qk + r$, where q is the quotient and r is the remainder (so $0 \leq r \leq k-1$).

   (b) $g^{kq} = (g^k)^q = e^q = e$.

   (c) Since $g^m = e$, we have $g^{kq+r} = e$, i.e. $g^{kq}\sigma^r = e$. Since $g^{kq} = e$ by the previous question, we get $g^r = e$.

   (d) What happens if $r > 0$? Since $r \leq k - 1$, we obtain that r is a positive integer smaller than k with the property that $g^r = e$. But by definition of the order of g, k is the smallest positive integer such that $g^k = e$, so $r > 0$ is not possible and we must have $r = 0$.

   (e) From the previous question we obtain $r = 0$, so $m = kq$, in other words m is a multiple of k.

4. (a) $\sigma^N = (\sigma_1 \cdots \sigma_k)^N = \sigma_1^N \cdots \sigma_k^N$ (because the cycles $\sigma_1, \ldots, \sigma_k$ are disjoint, so we can change the order of the terms in their product, so we can put all the σ_1 together, all the σ_2 together, etc.). But by definition N is a multiple of the order of each σ_i: $N = k_i|\sigma_i|$ for some $k_i \in \mathbb{N}$. Therefore $\sigma_i^N = \sigma_i^{k_i|\sigma_i|} = (\sigma_i^{|\sigma_i|})^{k_i} = \mathrm{id}^{k_i} = \mathrm{id}$ for every i. Thus we obtain $\sigma^N = \mathrm{id}\,\mathrm{id}\cdots\mathrm{id} = \mathrm{id}$.

   (b) This is the harder question. There are many ways to write an answer to it. The following is just one way to do it. Let A_i be the set of elements that appear in the cycle notation of σ_i. By definition of cycle, σ_i only moves the elements of A_i and not the others. Also, since the cycles $\sigma_1, \ldots, \sigma_k$ are disjoint, the sets $A_1, \ldots, A_k$ are disjoint (it is exactly the definition of disjoint cycles). In particular there are no elements in A_1 and in $A_2 \cup \cdots \cup A_k$ (we will use that below).

By definition of σ_1 and A_1, we know that $\sigma_1^{r_1}$ only moves elements of A_1. But $\sigma_2^{r_2} \cdots \sigma_k^{r_k}$ only moves elements that are in $A_2 \cup \cdots \cup A_k$. Since $\sigma_1^{r_1} = \sigma_2^{r_2} \cdots \sigma_k^{r_k}$ we get that $\sigma_1^{r_1}$ only moves elements that are in both A_1 and $A_2 \cup \cdots \cup A_k$. As observed above, there are no such elements, so $\sigma_1^{r_1}$ does not move any elements, so is the identity map.

(c) Since $\sigma^t = \mathrm{id}$ (and $\sigma_1, \ldots, \sigma_k$ are disjoint cycles) we have $\sigma_1^t \sigma_2^t \cdots \sigma_k^t = \mathrm{id}$. Therefore $\sigma_1^t = (\sigma_2^t \cdots \sigma_k^t)^{-1} = (\sigma_k^t)^{-1} \cdots (\sigma_2^t)^{-1} = \sigma_k^{-t} \cdots \sigma_2^{-t} = \sigma_2^{-t} \cdots \sigma_k^{-t}$ (the last equality uses that the cycles are disjoint and thus that we can reorder as we want the elements in the product). By the previous question we obtain $\sigma_1^t = \mathrm{id}$.

The same reasonning using $\sigma_2, \ldots, \sigma_k$ instead of σ_1 would give $\sigma_2^t = \mathrm{id}$, ..., $\sigma_k^t = \mathrm{id}$.

(d) Since $\sigma_i^t = \mathrm{id}$ for every i we know by exercise 4 that t is a multiple of t_i (since $t_i = |\sigma_i|$).

(e) By the previous question, t is a multiple of $t_1, \ldots, t_k$, so is a multiple of $\mathrm{lcm}(t_1, \ldots, t_k) = N$. In particular $t \geq N$. But $\sigma^N = \mathrm{id}$ and by definition t is the smallest positive integer such that $\sigma^t = \mathrm{id}$. The only possibility is $t = N$. In other words:

$$|\sigma| = \mathrm{lcm}(|\sigma_1|, \ldots, |\sigma_k|).$$