Homework exercise sheet 3

Due 12:50pm, Friday 12th February 2010

1. Insert the word "odd" or "even" in the gaps and prove the resulting statements.

   (a) The product of two even permutations is _________.

   (b) The product of three odd permutations is _________.

   (c) The product of an even and an odd permutation is _________.

   Solution (a) The product of two even permutations is even, since if α, β are even permutations then $\sigma(\alpha \circ \beta) = \sigma(\alpha) \cdot \sigma(\beta) = 1 \cdot 1 = 1$.

   (b) The product of three odd permutations is odd since if α, β, γ are odd permutations then $\sigma(\alpha \circ \beta \circ \gamma) = \sigma(\alpha) \cdot \sigma(\beta \circ \gamma) = \sigma(\alpha) \cdot \sigma(\beta) \cdot \sigma(\gamma) = (-1) \cdot (-1) \cdot (-1) = -1$.

   (c) The product of an even and an odd permutation is odd since if α is even and β is odd then $\sigma(\alpha \circ \beta) = \sigma(\alpha) \cdot \sigma(\beta) = 1 \cdot (-1) = -1$ and $\sigma(\beta \circ \alpha) = \sigma(\beta) \cdot \sigma(\alpha) = (-1) \cdot 1 = -1$. [We do need both parts for a complete proof here].

2. Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 2 & 1 & 7 & 6 & 3 \end{pmatrix}$ as a product of disjoint cycles. Determine whether this permutation is odd or even using two different methods: by counting inversions, and by examining your product of disjoint cycles.

   Solution We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 2 & 1 & 7 & 6 & 3 \end{pmatrix} = (1\ 4\ 2\ 5)(3\ 8)(6\ 7)$. There are 15 inversions in this permutation, so it is odd. Alternatively, each of the three cycles $(1\ 4\ 2\ 5)$, $(3\ 8)$ and $(6\ 7)$ has even length, so they are all odd permutations. Hence their product is odd.

3. Consider the permutation in S_{10} given by

   $$\alpha = (4\ 2\ 1)(5\ 4\ 9\ 10)(2\ 3\ 4)(7\ 1)(3\ 6).$$

   Without rewriting α, compute $\sigma(\alpha)$. Then write α in 2-row notation and as a product of disjoint cycles.

   Solution We have

   $$\sigma(\alpha) = \sigma(4\ 2\ 1)\sigma(5\ 4\ 9\ 10)\sigma(2\ 3\ 4)\sigma(7\ 1)\sigma(3\ 6) = 1 \cdot (-1) \cdot 1 \cdot (-1) \cdot (-1) = -1.$$

   Using the usual rules for composing permutations (working from right to left) gives

   $$\alpha = (1\ 7\ 4)(2\ 3\ 6\ 9\ 10\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 3 & 6 & 1 & 2 & 9 & 4 & 8 & 10 & 5 \end{pmatrix}.$$

4. (a) Let $n, k \in \mathbb{N}$, let $a_1, a_2, \ldots, a_k$ be distinct elements of $\{1, 2, \ldots, n\}$, and consider the cycle $\alpha = (a_1\ a_2\ \ldots\ a_k)$ in S_n. What is α^{-1}?

   [As always, prove that your answer is correct].

   (b) If $(G, *)$ is a group and $x_1, x_2, \ldots, x_n \in G$, then the following identity holds:

   $$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1} * x_1^{-1}.$$

   Consider the following permutation in S_{16}:

   $$\alpha = (11\ 7)(1\ 3\ 15\ 2\ 4)(6\ 12\ 13\ 9)(5\ 8).$$

   Use (a) and the identity above to compute α^{-1}, writing your answer as a product of disjoint cycles.

Solution Recall that $\alpha(a_i) = a_{i+1}$ if $1 \le i < k$, and $\alpha(a_k) = a_1$, and $\alpha(x) = x$ if $x \notin \{a_1, \dots, a_n\}$.

Let $\beta = (a_k\ a_{k-1}\ \dots\ a_2\ a_1)$. Then $\beta(a_i) = a_{i-1}$ if $1 < i \le k$, and $\beta(a_1) = a_k$, and $\beta(x) = x$ if $x \notin \{a_1, \dots, a_k\}$.

If $x \in \{1, 2, \dots, n\}$ with $x \notin \{a_1, \dots, a_n\}$ then $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \beta(x) = x$ and $(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$.

If $x = a_i$ for some i with $1 < i < k$, then $(\beta \circ \alpha)(x) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_i = x$ and $(\alpha \circ \beta)(x) = \alpha(\beta(a_i)) = \alpha(a_{i-1}) = a_i = x$.

If $x = a_1$ then $(\beta \circ \alpha)(x) = \beta(\alpha(a_1)) = \beta(a_2) = a_1 = x$ and $(\alpha \circ \beta)(x) = \alpha(\beta(a_1)) = \alpha(a_k) = a_1 = x$.

If $x = a_k$ then $(\beta \circ \alpha)(x) = \beta(\alpha(a_k)) = \beta(a_1) = a_k = x$ and $(\alpha \circ \beta)(x) = \alpha(\beta(a_k)) = \alpha(a_{k-1}) = a_k = x$.

Hence for every $x \in \{1, 2, \dots, n\}$, we have $(\beta \circ \alpha)(x) = x = e(x)$ and $(\alpha \circ \beta)(x) = x = e(x)$ where e is the identity element of S_n. So $\beta \circ \alpha = e$ and $\alpha \circ \beta = e$. So $\alpha^{-1} = \beta = (a_k\ a_{k-1}\ \dots\ a_2\ a_1)$.

(b) By the identity in the question, taking $x_1 = (11\ 7)$, $x_2 = (1\ 3\ 15\ 2\ 4)$, $x_3 = (6\ 12\ 13\ 9)$ and $x_4 = (5\ 8)$, we have

$$\alpha^{-1} = \big((11\ 7)(1\ 3\ 15\ 2\ 4)(6\ 12\ 13\ 9)(5\ 8)\big)^{-1} = (5\ 8)^{-1}(6\ 12\ 13\ 9)^{-1}(1\ 3\ 15\ 2\ 4)^{-1}(11\ 7)^{-1}.$$

Inverting each of these cycles using (a) gives $\alpha^{-1} = (8\ 5)(9\ 13\ 12\ 6)(4\ 2\ 15\ 3\ 1)(7\ 11)$, and this is a product of disjoint cycles.

5. Let $n \in \mathbb{N}$, and let α be the cycle in S_n given by $\alpha = (1\ 2\ \dots\ n)$. For $k \in \mathbb{N}$, let us write

$$\alpha^k = \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{k\,\text{times}},$$

and let us also write $\alpha^0 = e$ where e is the identity mapping in S_n.

(a) Show that $\alpha^n = e$ and that $\alpha^s \circ \alpha^t = \alpha^{s+t}$ for any integers $s, t \ge 0$.
(b) Show that if s, t are integers with $0 \le s, t < n$ and $\alpha^s = \alpha^t$, then $s = t$.
(c) Prove that composition is an operation on the set $C_n = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, and deduce that $(C_n, \circ)$ is an abelian group of order n.
(d) Write down the Cayley tables of the groups $(C_n, \circ)$ for $n = 1, 2, 3, 4$.

Solution (a) Since α is a cycle of length n, it is easy to see that $\alpha^n(x) = x$ for all $x \in \{1, 2, \dots, n\}$ [for example, by drawing a picture]. Hence $\alpha^n = e$.

By the associativity of composition, we have

$$\alpha^s \circ \alpha^t = (\underbrace{\alpha \circ \cdots \circ \alpha}_{s\,\text{times}}) \circ (\underbrace{\alpha \circ \cdots \circ \alpha}_{t\,\text{times}}) = \underbrace{\alpha \circ \cdots \circ \alpha}_{s+t\,\text{times}} = \alpha^{s+t}$$

for $s, t \ge 1$. Since $\alpha^0 = e$, this equation clearly also holds if either s or t is zero, hence it is true for all integers $s, t \ge 0$.

(b) Observe that $\alpha^s(1) = s+1$ and $\alpha^t(1) = t+1$ for $0 \le s,t < n$. If $\alpha^s = \alpha^t$ then this implies that $s+1 = t+1$, so $s = t$.

(c) To see that $\circ$ is an operation on $C_n = \{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$, we must show that $\beta, \gamma \in C_n \implies \beta \circ \gamma \in C_n$. So let $s, t \in \{0, 1, \ldots, n-1\}$ and consider $\beta = \alpha^s$ and $\gamma = \alpha^t$. If $s + t < n$ then $\beta \circ \gamma = \alpha^s \circ \alpha^t = \alpha^{s+t} \in C_n$. If $s + t \ge n$ then we have $n \le s + t < 2n$, so $0 \le s + t - n < n$, and

$$\beta \circ \gamma = \alpha^{s+t} = \alpha^{s+t-n} \circ \alpha^n = \alpha^{s+t-n} \circ e = \alpha^{s+t-n} \in C_n.$$

Hence, in either case, $\beta \circ \gamma \in C_n$, so $\circ$ is an operation on C_n.

To see that $(C_n, \circ)$ is a group:

- $\circ$ is associative on S_n, so it is certainly associative on C_n
- $e \in C_n$ and it is the identity element for all of S_n, so it is an identity element for C_n
- if $\beta \in C_n$ then $\beta = \alpha^s$ for some integer s with $0 \le k < n$, and $\gamma = \alpha^{n-s}$ satisfies $\beta \circ \gamma = \alpha^n = \gamma \circ \beta$, so $\gamma = \beta^{-1}$ and $\gamma \in C_n$ (in the case $s = 0$, this is because $\alpha^n = e \in C_n$).

To see that $(C_n, \circ)$ is an abelian group, observe that if $\beta, \gamma \in C_n$ then $\beta = \alpha^s$ and $\gamma = \alpha^t$ for some integers $s, t \ge 0$, so

$$\beta \circ \gamma = \alpha^s \circ \alpha^t = \alpha^{s+t} = \alpha^{t+s} = \alpha^t \circ \alpha^s = \gamma \circ \beta.$$

By (b), no two of the mappings $e, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are equal. Hence the order of C_n is $|C_n| = n$.

(d) We have

$n = 1$:

$\circ$	e
e	e

$n = 2$:

$\circ$	e	α
e	e	α
α	α	e

$n = 3$:

$\circ$	e	α	α^2
e	e	α	α^2
α	α	α^2	e
α^2	α^2	e	α

$n = 4$:

$\circ$	e	α	α^2	α^3
e	e	α	α^2	α^3
α	α	α^2	α^3	e
α^2	α^2	α^3	e	α
α^3	α^3	e	α	α^2