HW 3
Due: Tuesday, February 18

Do exercises 2/22, 24, 26ii and iii, 27, 28, 30, 31, and the following:

A. Let $\sigma = (4\,5\,2\,1)(3\,6\,7)$ and $\tau = (1\,3\,4)(2\,5)$. Compute $\sigma\tau$ and $\tau\sigma$.

B. With notation as above, compute $\sigma\tau\sigma^{-1}$.

C. Find $\alpha \in S_7$ for which
$$\alpha\tau\alpha^{-1} = (1\,2\,3)(4\,5).$$

D. Find the smallest positive k such that $\sigma^k = (1)$.

Change

Chapter 2 Solutions

Proposition 1 (Exercise 2.22)**.** *Let $\alpha \in S_n$ be a permutation.*

(i) If α is an r-cycle then $\alpha^r = (1)$.

(ii) Additionally, r is the smallest positive integer such that $\alpha^k = (1)$.

Proof. (i) Let $i_0, i_1, ...$ (where this list is infinite) be integers in $\{1, ..., n\}$ such that $i_{j+1} = \alpha(i_j)$ for each $j \in \mathbb{N}$, where $i_0, ..., i_{r-1}$ are distinct and we define $i_p = i_q$ if $p \equiv q \bmod r$.

We claim that

$$\alpha^k(i_j) = i_{j+k} \tag{1}$$

for all $k, j \in \mathbb{N}$.

Then we proceed with a proof by induction on k.

Fix $j \in \mathbb{N}$. Let $k = 1$. Then

$$\alpha^k(i_j) = \alpha^1(i_j) = i_{j+1},$$

by choice of α.

Now suppose that $k > 1$. We assume that,

$$\alpha^t(i_j) = i_{j+t}.$$

for all t satisfying $1 \leq t < k$. By choice of α and the induction hypothesis we have the following:

$$\begin{aligned} \alpha^k(i_j) &= \alpha(\alpha^{k-1}(i_j)) \\ &= \alpha(i_{j+k-1}) \\ &= i_{j+k}. \end{aligned}$$

Therefore, by induction our claim holds for all $k \in \mathbb{Z}^+$. This result then holds for all $j \in \mathbb{Z}^+$, because j was chosen to be arbitrary. We observe that α then operates as addition on the indices of $\{i_0, ..., i_{r-1}\}$.

Suppose that $i_j \in \{i_0, ..., i_{r-1}\}$. We note that α is an r-cycle. By our choice of indices,

$$\alpha^r(i_j) = i_{j+r} = i_j.$$

Since j was chosen to be arbitrary, it follows that $\alpha^r = (1)$.

(ii) Assume that α is as in part (i). For $r = 1$, r is then the smallest positive integer. Thus, the claim must hold. Assume that $r > 1$. Let k be some other integer such that $\alpha^k = (1)$. For the sake of contradiction, assume that $k < r$. Thus, for any

$j \in \mathbb{Z}^+$, $\alpha^k(i_1) = i_{1+k}$, by our claim. So, $i_{1+k} = i_1$ by hypothesis. We observe that $1 \leq k+1 \leq r$ by choice of k. Thus, we have that $i_1, ..., i_{k+1}, ..., i_r$ are not all distinct. But this contradicts our choice of $i_1, ..., i_r$. So, no such k must exist. Therefore, r is the smallest positive integer satisfying $\alpha^r = (1)$. ■

Proposition 2 (Exercise 2.24)**.** *Given $X = \{1, 2, ..., n\}$, let us call a permutation τ of X an adjacency if it is a transposition of the form*

$$(i \;\; i+1)$$

for $i < n$. Let $\tau = (ij)$. If $i < j$, then τ is a product of an odd number of adjacencies.

Proof. Fix $i, j \in X$. Since τ is a 2-cycle, it follows that τ has $n-1$ factors in its complete factorization. We observe that

$$\text{sgn}(\tau) = (-1)^{n-(n-1)} = (-1)^1 = -1.$$

Hence, τ is odd. By Theorem 2.40, τ is a product of an odd number of transpositions. Similarly, any adjacency is a transposition, so if τ is a product of adjacencies then τ must be a product of an odd number of adjacencies by Theorem 2.40. Hence, it suffices to show that τ is a product of adjacencies.

Let $k = j - i$. We wish to show that when $k \geq 2$, the following equality holds:

$$(i \;\; j) = \prod_{n=i}^{j-1} (n \;\; n+1) \prod_{n=j-1}^{i+1} (n-1 \;\; n).$$

We note that when $k = 1$, then τ is trivially a product of adjacencies.

Let $k = 2$. Then

$$(i \;\; j) = (i+1 \;\; i)(i+1 \;\; j)(i \;\; i+1) \tag{2}$$

This can be seen by directly plugging in the values $i, i+1, j$ into the right hand side. From which we get the following strings of outputs:

$$i \mapsto i+1 \mapsto j \mapsto j,$$

$$i+1 \mapsto i \mapsto i \mapsto i+1,$$

and

$$j \mapsto j \mapsto i+1 \mapsto i.$$

Since $(i \;\; j)$ and the RHS of equation 2 fix every element that is not one of $i, i+1, j$ we see that the equality holds.

Let $k > 2$. Then we assume

$$(r \;\; s) = \prod_{n=r}^{s-1} (n \;\; n+1) \prod_{n=s-1}^{r+1} (n-1 \;\; n). \tag{3}$$

for all integers $r, s \in X$ such that $r < s$ and $s - r \leq k - 1$. Note that transpositions are their own inverses, so $(r \;\; s) = (s \;\; r)$.

We claim that

$$
\begin{aligned}
&(i \;\; j) = (j-1 \;\; i)(j-1 \;\; j)(i \;\; j-1) \\
&= \Big(\prod_{n=i}^{j-2}(n \;\; n+1) \prod_{n=j-2}^{i+1}(n-1 \;\; n)\Big)(j-1 \;\; j)\Big(\prod_{n=i}^{j-2}(n \;\; n+1) \prod_{n=j-2}^{i+1}(n-1 \;\; n)\Big) \\
&= \Big(\prod_{n=i}^{j-1}(n \;\; n+1) \prod_{n=j-2}^{i+1}(n-1 \;\; n)\Big)\Big(\prod_{n=i}^{j-2}(n \;\; n+1) \prod_{n=j-2}^{i+1}(n-1 \;\; n)\Big) \\
&= \Big(\prod_{n=i}^{j-1}(n \;\; n+1) \prod_{n=j-2}^{i+1}(n-1 \;\; n)\Big)\Big(\prod_{n=i}^{j-3}(n \;\; n+1) \prod_{n=j-1}^{i+1}(n-1 \;\; n)\Big) \\
&= \Big(\prod_{n=i}^{j-1}(n \;\; n+1)\Big)\Big(\prod_{n=j-2}^{i+1}(n-1 \;\; n)\prod_{n=i}^{j-3}(n \;\; n+1)\Big)\Big(\prod_{n=j-1}^{i+1}(n-1 \;\; n)\Big) \\
&= \Big(\prod_{n=i}^{j-1}(n \;\; n+1)\Big)\Big(1\Big)\Big(\prod_{n=j-1}^{i+1}(n-1 \;\; n)\Big) \\
&= \Big(\prod_{n=i}^{j-1}(n \;\; n+1) \prod_{n=j-1}^{i+1}(n-1 \;\; n)\Big).
\end{aligned}
$$

It's clear the first equality holds by an argument similar to the argument in the $k = 2$ case. The second equality holds by the induction hypothesis. The third equality holds since disjoint cycles commute. The fourth equality holds because of the associativity of function composition. The fifth equality holds, also, by associativity of function composition. The sixth equality holds because each transposition is its own inverse. The seventh equality holds again by the associativity of function composition.

Thus, our claim holds by induction. Moreover, $(i \;\; j)$ is then a product of adjacencies and we conclude that the proposition holds. ■

Proposition 3 (Exercise 2.26 ii,iii)**.** *Let $\alpha \in S_n$.*

(i) Prove that if α is an r-cycle, then α^k is a product of $gcd(r,k)$ disjoint cycles, each of length $r/gcd(r,k)$.

(ii) If p is a prime, prove that every power of a p-cycle is either a p-cycle or (1).

Proof. (i) Since α is an r-cycle, α moves r elements in $1, ..., n$. We label the elements moved by α as $i_0, ..., i_{r-1}$. Moreover, define $\alpha(i_j) = i_{j+1}$ and say that $i_p = i_q$ if $p \equiv q \bmod r$ for all $j, p, q \in \mathbb{N}$. By our claim above, (1), in the proof of Proposition 1, we see that $\alpha^b(i_j) = i_{j+b}$ for any $b \in \mathbb{N}$.

Fix $i_j \in \{i_0, ..., i_{r-1}\}$. Set $d = gcd(r,k)$ and $m = lcm(r,k)$. We observe that $r|m$. Then

$$(\alpha^k)^{\frac{r}{d}}(i_j) = i_{j+\frac{rk}{d}} = i_{j+m} = i_j.$$

by choice of α. We also give α^k the following complete factorization of disjoint cycles:

$$\alpha^k = \beta_1, ..., \beta_t.$$

We discard any 1-cycles in this factorization and relabel such that t counts the number of a-cycles in this factorization with $a > 1$. Say that each cycle has length r_i with $1 \leq i \leq t$. It still holds that $t < n$. If anything t is now smaller. Then there exists some disjoint cycle in the factorization of α^k, say β_b, such that $\alpha^k(i_j) = \beta_b(i_j)$. Thus, $(\alpha^k(i_j))^{\frac{r}{d}} = \beta_b^{\frac{r}{d}}(i_j) = i_j$. Observe that for any other element $i_{j'}$ that is moved by β_b we could argue, using a similar argument to that above, to say that $\beta_b^{\frac{r}{d}}(i_{j'}) = i_{j'}$. Since β_b fixes every other element in $\{1, ..., n\}$, $\beta_b^{\frac{r}{d}} = (1)$. We observe that the factorization of α^k was chosen such that each cycle moves at least 2 elements in $\{i_0, ..., i_{r-1}\}$. Thus, this argument holds for all cycles in the complete factorization of α^k. By exercise 2.22 we know that the cycle length of any cycle in the factorization is the smallest power making that cycle (1). So, $\frac{r}{d}$ is at most the length of each cycle. Thus, there are at least d cycles. More precisely, $t \leq d$. Suppose that some cycle has length $\ell \leq \frac{r}{d}$. Since each cycle is disjoint, we observe that the sum of the lengths of the cycles must be r. In particular, say β_t has length ℓ. Thus,

$$r = (t-1)\frac{r}{d} + \ell \leq t\frac{r}{d} \leq d\frac{r}{d} \leq r.$$

So, it follows that these inequalities only hold when equality holds. Thus, $t = d$. Since $t = d$, and the lengths of the cycles sum to r, it follows that each cycle must have length $\frac{r}{d}$.

(ii) Suppose that α is a p-cycle for some prime p. From part (i), we observe that $\alpha^k = \beta_1 \cdots \beta_d$ where $d = gcd(p, k)$ for any $k \in \mathbb{Z}^+$. But $d = 1$, because p is prime. If k is a multiple of p then $\alpha^k = (1)$ by Exercise 2.22. If k is not a multiple of p, $\alpha^k = \beta_1$ is a p-cycle with length $\frac{p}{d} = p$.

■

Proposition 4 (Exercise 2.27)**.** *Let $\alpha, \beta \in S^n$.*

(i) Suppose that α and β commute. Then $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 1$.

(ii) There exists an example of α and β such that $(\alpha\beta)^k \neq \alpha^k\beta^k$.

Proof. (i) We proceed by induction on k. For $k = 1$, it follows immediately by hypothesis.

Suppose that $k > 1$. Then assume that, $(\alpha\beta)^t = \alpha^t\beta^t$ for each t such that $1 \leq t < k$.

$$\begin{aligned}(\alpha\beta)^k &= (\alpha\beta)^{k-1}(\alpha\beta)\\ &= \alpha^{k-1}\beta^{k-1}\alpha\beta\\ &= \alpha^{k-1}\alpha\beta^{k-1}\beta\\ &= \alpha^k\beta^k.\end{aligned}$$

The equality above holds because α commutes with β and so it commutes with every copy of β in β^{k-1}. Thus, the conclusion holds for all $k \in \mathbb{Z}^+$.

(ii) Choose $\alpha = (1234)$ and $\beta = (1324)$ from S^4.

$$(\alpha\beta)^2 = ((1234)(1324))^2 = ((142)(3))^2 = (142)(142) = (124)$$

Also,

$$\alpha^2 = (1234)(1234) = (13)(24)$$

and

$$\beta^2 = (1324)(1324) = (12)(34).$$

$$\alpha^2\beta^2 = (13)(24)(12)(34) = (14)(23).$$

Thus, $(\alpha\beta)^2 \neq \alpha^2\beta^2$. ■

Proposition 5 (Exercise 2.28)**.** *Suppose that α is a permutation in S^n. Then α moves $i \in \{1, ..., n\}$ if and only if α^{-1} moves i.*

Proof. Suppose that α has the following complete factorization into disjoint cycles:

$$\alpha = \beta_1 \cdots \beta_t.$$

By Proposition 2.27,

$$\alpha^{-1} = \beta_1^{-1} \cdots \beta_t^{-1}.$$

Choose some i that is moved by α. Then i is moved by some cycle in the factorization of α. WLOG, say β. Suppose that β is an r-cycle. We then give the symbols moved by β an index. In particular, we say that $i = i_0$, $i_{j+1} = \beta(i_j)$ and $i_p = i_q$ if $p \equiv q \bmod r$ for all $p, q, j \in \mathbb{N}$. Then we observe that

$$\beta^r = \beta\beta^{r-1} = \beta^{r-1}\beta = (1) \tag{4}$$

by Exercise 2.22. Thus, $\beta^{r-1} = \beta^{-1}$. From our claim (1) in the proof of Proposition 1, we observe that $\beta^{-1}(i_0) = i_{r-1}$. Since $r - 1 \not\equiv 0 \bmod r$, we have that $i_{r-1} \neq i_0$. From which it follows that β^{-1} moves i. Moreover, we see that $\alpha^{-1}(i) = \beta^{-1}(i)$, by (4) and the fact that the cycles in the factorization of α^{-1} are disjoint. Thus, α^{-1} moves i. Since i was chosen to be arbitrary, this argument will hold for any i that is moved by α. ■

Proposition 6 (Exercise 2.30)**.** *There exists $\alpha, \beta, \gamma \in S^5$, none of which is the identity,*

$$\alpha\beta = \beta\alpha, \qquad \textit{and} \qquad \alpha\gamma = \gamma\alpha$$

but

$$\beta\gamma \neq \gamma\beta.$$

Proof. Say that $\gamma = (12345)$ and $\beta = (123)$. Then

$$\gamma\beta = (13245)$$

$$\beta\gamma = (13452)$$

Choose $\alpha = (12)$.

$$\alpha\beta = (12)(12345) = (1)(2345) =$$

■

Proposition 7 (Exercise 2.31)**.** *Let $n \geq 3$. Supose that $\alpha \in S^n$. Then α commutes with every permutation in S^n if and only if $\alpha = (1)$.*

Proof. The reverse direction is obvious, because (1) is the identity function. So, it suffices to show the forward direction. Then we wish to show that α fixes every i in $\{1, ..., n\}$. In other words, we wish to show that α does not move any i in $\{1, ..., n\}$.

Assume for the sake of contradiction that α moves some symbol in the set $\{1, ..., n\}$. In particular, say that α moves i. This implies there is some symbol, say j, such that α sends $i \mapsto j$, and i and j are distinct. Since $n \geq 3$ there exists some symbol k in $\{1, ..., n\}$ where each of i, j and k are distinct. Choose $\beta \in S^n$ to be $\beta = (jk)$. Then,

$$(\beta\alpha)(i) = \beta(j) = k$$

and

$$(\alpha\beta)(i) = \alpha(i) = j.$$

But this contradicts the choice of α. Since we chose i to be arbitrary, α must not move any symbol in $\{1, ..., n\}$. It follows that α fixes every symbol. Thus, $\alpha = (1)$.

■

Non-text Solutions

Proposition 8 (Exercise A)**.** *Let $\sigma = (4521)(367)$ and $\tau = (134)(25)$. Compute $\sigma\tau$ and $\tau\sigma$.*

Proof. Then

$$\sigma\tau = (16735)(25)(4) = (16735)(25).$$

and

$$\tau\sigma = (1)(23674)(5) = (23674).$$

■

Proposition 9 (Exercise B)**.** *Leaving σ and τ as defined in Exercise A compute $\sigma\tau\sigma^{-1}$.*

Proof.

$$\sigma\tau\sigma^{-1} = (4521)(367)(134)(25)(1254)(763) = (12)(3)(465)(7) = (12)(456).$$

■

Proposition 10 (Exercise C)**.** *Find $\alpha \in S^7$ for which*

$$\alpha\tau\alpha^{-1} = (123)(45).$$

Proof. By Proposition 2.32, we see that we need some $\alpha \in S^n$ such that

$$\begin{aligned}\alpha(1) &= 1\\ \alpha(3) &= 2\\ \alpha(4) &= 3\\ \alpha(2) &= 4\\ \alpha(5) &= 5.\end{aligned}$$

Thus, $\alpha = (1)(324)(5) = (324)$. As a check:

$$\alpha\tau\alpha^{-1} = (324)(134)(25)(423) = (123)(45).$$

■

Proposition 11 (Exercise D)**.** *Find the smallest positive k such that $\sigma^k = (1)$.*

Proof. By the exercise 2.22, $(367)^3 = (1)$ and $(4521)^4 = (1)$. It follows that this occurs are every multiple of 3 and 4, respectively. Thus, $\sigma^k = (1)$ when k is a common multiple of both 3 and 4. Then the smallest integer such that this occurs is the $lcm(3, 4) = 12$. Hence, $k = 12$. ■