HOMEWORK 3 (DUE: 11:15 AM, OCT 3 WED)

1. Do Exercise 7.A.1–5. in [Pin10, p. 75]. You do not need to justify your answers.

7.A.1. We have

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} \qquad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$$

$$h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix} \qquad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 6 & 3 \end{pmatrix}$$

7.A.2. $f \circ (g \circ h) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 2 & 4 & 3 \end{pmatrix}$

7.A.3. $g \circ h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 5 & 1 \end{pmatrix}$

7.A.4. $h \circ g^{-1} \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$

7.A.5. $g \circ g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$

2. Do Exercise 7.E.1–4. in [Pin10, p. 77]. Here you *need* to justify your answers.

7.E.1. It is clear that $f_{a,b}$ is a function from $\mathbb{R}$ to $\mathbb{R}$. Now consider another function $f_{1/a,-b/a}$ (which is well-defined since $a \neq 0$). Then for any $x \in \mathbb{R}$, we have

$$(f_{a,b} \circ f_{1/a,-b/a})(x) = f_{a,b}(\frac{x-b}{a}) = x, \qquad (f_{1/a,-b/a} \circ f_{a,b})(x) = f_{1/a,-b/a}(ax+b) = x,$$

thus $f_{a,b}$ and $f_{1/a,-b/a}$ are inverse to each other. Since $f_{a,b}$ has an inverse, we see that $f_{a,b}$ is a bijection, i.e. permutation of $\mathbb{R}$.

7.E.2. For any $x \in \mathbb{R}$, we have

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx+d) = acx + ad + b = f_{ac,ad+b}(x).$$

Therefore $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$.

7.E.3. We already showed this in part 1).

7.E.4. By 2), G is closed under composition. By 3), G is closed by taking inverses. Also, the identity map $id_{\mathbb{R}} = f_{1,0}$ is in G. Thus G is a subgroup of $S_{\mathbb{R}}$.

3. Do Exercise 8.A.1–3. (*not all of 1–6!*) in [Pin10, p. 86]. You do not need to justify your answers.

8.A.1. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 7 & 5 & 1 & 8 & 3 & 2 & 9 \end{pmatrix} = (145)(268)(37)$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 5 & 9 & 4 & 2 & 1 & 6 & 3 \end{pmatrix} = (17)(286)(3549)$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 6 & 9 & 7 & 3 & 1 & 2 & 4 \end{pmatrix} = (18257)(36)(49)$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 7 & 5 & 6 & 3 & 8 & 9 \end{pmatrix} = (12)(347)$

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 6 & 5 & 1 & 7 & 4 & 9 \end{pmatrix} = (132846)$

(f) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 9 & 2 & 1 & 7 & 6 & 8 \end{pmatrix} = (134986)(25)$

8.A.2. (a) $(145)(293)(67)$

(b) $(17)(24)(395)(68)$

(c) $(17435)(296)$

(d) $(1928)(375)$

8.A.3. (a) $(18)(12)(14)(17)(13)$

(b) $(16)(14)(28)(25)(23)$

(c) $(13)(12)(14)(16)(57)$

(d) $(12)(14)(13)(58)(67)$

4. Do Exercise 8.B.5–8. (*not all of 1–8!*) in [Pin10, p. 87]. Here you *need* to justify your answers.

Before we proceed, we prove the following lemma.

Lemma 0.1. *Let $\alpha \in S_n$ be a cycle of length s. Then for any $k \in \mathbb{Z}$, α^k is a product of $\gcd(s,k)$ disjoint cycles of length $\frac{s}{\gcd(s,k)}$.*

Proof. After relabeling elements in $\{1, 2, \ldots, n\}$, without loss of generality we may assume that $\alpha = (0123 \cdots (s-1)) \in S_n$. Then it is clear that for any $m \in \mathbb{Z}$ and for any $0 \leq i \leq s-1$ we have

$$\alpha^m(i) = i + m \mod s$$

Let us write $g = \gcd(s, k)$ for brevity. We claim that

$$\{\alpha^{mk}(0) \in \{0, 1, \ldots, s-1\} \mid m \in \mathbb{Z}\} = \{\alpha^{mg}(0) \in \{0, 1, \ldots, s-1\} \mid m \in \mathbb{Z}\},$$

or in other words

$$\{mk \mod s \mid m \in \mathbb{Z}\} = \{mg \mod s \mid m \in \mathbb{Z}\}.$$

Note that $\subset$ direction is clear, since multiples of k are also multiples of g. On the other hand, By Euclidean algorithm there exists $a, b \in \mathbb{Z}$ such that $as + bk = g$. Therefore

$$mg = ams + bmk \equiv bmk \mod s,$$

which means that multiplies of g modulo s are contained in the set of multiples of k modulo s. This means $\supset$ direction and the claim follows.

Therefore, the orbits of α^k on the set $\{0, 1, \ldots, s-1\}$ is given by

$$\{0, g, 2g, \ldots, s-g\}, \{1, g+1, 2g+1, \ldots, s-g+1\}, \ldots, \{g-1, 2g-1, \ldots, s-1\}.$$

There are exactly g number of orbits of size s/g. This proves the lemma. □

8.B.5. Since $\gcd(s, s+1) = 1$, also $\gcd(s, (s+1)/2) = 1$,, which means that $\alpha^{(s+1)/2}$ is a cycle of length s by the lemma above. Now $\alpha = \alpha^{s+1} = (\alpha^{(s+1)/2})^2$. (Note that the order of α is s, we will prove it in the exercise below.)

8.B.6. Since $\gcd(s, 2) = 2$ by assumption, α^2 is the product of two cycles of length $t = s/2$ by lemma above. If we write $\alpha = (a_1 a_2 \cdots a_s)$ then we have

$$\alpha^2 = (a_1 a_3 a_5 \cdots a_{s-1})(a_2 a_4 a_6 \cdots a_s).$$

8.B.7. Since $\gcd(s, k) = k$ by assumption, it follows from the lemma above.

8.B.8. Let $k \in \mathbb{Z}$. If $\gcd(s, k) = 1$ then α^k is a cycle of length s. Otherwise, since s is a prime we have $\gcd(s, k) = s$, i.e. k is a multiple of s. But then $\alpha^k = id$ which is an empty cycle since the order of α is s.

5. Do Exercise 8.F.1–5. in [Pin10, p. 88]. Follow the instructions.

8.F.1. We first prove that the order of α is s. It is clear that α^s maps each a_i to itself by the definition of cycles. Thus $\alpha^s = id$. On the other hand, if $1 \leq k < s$ then $\alpha^k(a_1) = a_{k+1} \neq a_1$, thus $\alpha^k \neq id$. Thus s is the order of α. Now it is clear that $\alpha^s = \alpha^{2s} = \alpha^{3s} = id$, and $\alpha^k \neq id$ if $1 \leq k < s$.

8.F.2. We already proved it above.

8.F.3. Let us prove more general statement:

Lemma 0.2. *Suppose that $\alpha \in G, \beta \in H$ so that $(\alpha, \beta) \in G \times H$. Then $|(\alpha, \beta)| = \mathrm{lcm}(|\alpha|, |\beta|)$.*

Proof. Let us write $m = |(\alpha, \beta)|$, $l = \mathrm{lcm}(|\alpha|, |\beta|)$ for brevity. First it is clear that $(\alpha, \beta)^l = (\alpha^l, \beta^l) = id$, thus $m \leq l$ by the definition of order. On the other hand, $(\alpha, \beta)^m = id$ if and only if $\alpha^m = id$ and $\beta^m = id$, thus m is the multiple of both $|\alpha|$ and $|\beta|$, which means $m \geq l$. It follows that $m = l$. □

In general, if two cycles $\alpha = (a_1 a_2 \cdots a_s)$ and $\beta = (b_1 b_2 \cdots b_t)$ are disjoint, then we may regard $\alpha \in S_s$, $\beta \in S_t$ where S_s is the group permuting $\{a_1, a_2, \ldots, a_s\}$ and S_t is the group permuting $\{b_1, b_2, \ldots, b_t\}$. Then $(\alpha, \beta) \in S_s \times S_t$ has order $\mathrm{lcm}(s, t)$. Furthermore, if we regard $S_s \times S_t$ as a subgroup of S_n permuting $\{1, 2, \ldots, n\}$, then $(\alpha, \beta) \in S_s \times S_t \subset S_n$ is nothing but the product of two disjoint cycles α and β. Therefore, by the lemma above we see that

$$|\alpha\beta| = \mathrm{lcm}(|\alpha|, |\beta|).$$

Let us use this fact to solve this exercise.

(a) $\mathrm{lcm}(2, 3) = 6$

(b) $\mathrm{lcm}(2, 4) = 4$

(c) $\mathrm{lcm}(4, 5) = 20$

8.F.4. $\mathrm{lcm}(4, 6) = 12$

8.F.5. $\mathrm{lcm}(r, s)$

References

[Pin10] Pinter, C. C., *A Book of Abstract Algebra*, 2nd ed., Dover Publications, 2010.