Homework 2

Elliott Yoon

October 2, 2023

1 9/25

1. Let $f = (a_1 \cdots a_k)$ be a cycle of length k in S_n. Write the inverse of f as a cycle.

   - f sends $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{k-1} \mapsto a_k, a_k \mapsto a_1$. To invert f, we need to map $a_1 \mapsto a_k, a_k \mapsto a_{k-1}, \ldots, a_2 \mapsto a_1$. The inverse of f can be written as $(a_1\, a_k\, a_{k-1} \cdots a_2)$. $\square$

2. Let $f = (a_1 \cdots a_k)$ be a cycle of length k in S_n. Prove that f has order k.

   - Notice that for any $1 \le i \le k$,
   $$f(a_i) = \begin{cases} a_{i+1} & i < k \\ a_1 & i = k \end{cases}.$$
   Similarly,
   $$f^n(a_i) = a_{1+(i+n-1 \mod k)}.$$
   Since $|f|$ is the smallest $m > 0$ such that $i - 1 \equiv i + m - 1 \mod k$ for all $1 \le i \le k$, we have that $m = k$. $\square$

3. Let $f = (a_1 \cdots a_k)$ be a cycle of length k in S_n. Fix $s \ge 1$. Find (and prove) necessary and sufficient conditions for f^s to be a cycle. Hint: first consider the case of $s = 2$.

   - We will show that f^s is a cycle exactly when either (a) k divides s or (b) $\gcd(k, s) = 1$.
     (a) Recall that $f^k = e$, where e is the identity in S_n. Suppose $k|s$. Then, we can write $s = nk$, where $n \in \mathbb{N}$, so
     $$f^s = f^{nk} = (f^k)^n = e^n = e,$$
     which is by definition a cycle.
     (b) Suppose $\gcd(k, s) = 1$. For all $m, n \in \{1, \ldots, k\}$, $m > n$, suppose for contradiction that there exist $p, q \in \mathbb{N}$ such that
     $$ms + 1 - kp = ns + 1 - kq.$$
     Thus $ms - ns = kp - kq = k(p - q)$, so k divides $(m - n)s$. Since k does not divide s by assumption, k must divide $m - n$. But $1 \le m \le k$ and $1 \le n \le k$, so $m - n \le k - n < k$ and thus $m - n < k$, a contradiction with $k|m - n$. Thus, it must be the case that
     $$ms + 1 \mod k \ne ns + 1 \mod k$$
     for all $m, n \in \{1, \ldots, k\}, m > n$. Thus $\{js + 1 \mod k \mid 1 \le j \le k\} = \{1, \ldots, k\}$ and
     $$\{f^s(a_{js+1}) \mid 0 \le j < k\} = \{a_1, \ldots, a_k\}$$

(c) Finally, suppose that $1 < \gcd(k, s) < k$, denoting $m = \gcd(k, s)$, and suppose also that f^s is a cycle. Then

$$(f^s)^{\frac{k}{m}} = f^{\frac{sk}{m}} = (f^k)^{\frac{s}{m}} = e,$$

so if $f^s = \{b_1, \ldots, b_l\}$, then $l \leq \frac{k}{m}$. Thus, there are at most $\frac{k}{m}$ elements x of $\{a_1, \ldots, a_k\}$ where $f^s(x) \neq x$. But all a_j satisfy $f^s(a_j) \neq a_j$ since $s \not\equiv 0 \mod k$ for $1 \leq j \leq k$, a contradiction. So f^s is not a cycle.

□

4. Let $\mathbb{Z}/N = \{0, \ldots, N-1\}$. Equip $\mathbb{Z}/N$ with the binary operation given by multiplication modulo N, so that if $a, b \in \mathbb{Z}/N$, then $a \cdot_N b = r$ where $ab = qN + r$ where $r \in \{0, \cdots N-1\}$. We write $ab \equiv r \mod N$. Let $(\mathbb{Z}/N)^\times \subseteq \mathbb{Z}/N$ be the subset of elements $a \in \mathbb{Z}/N$ such that there exists $b \in \mathbb{Z}/N$ with $ab \equiv ba \equiv 1 \mod N$.

   (a) Show that this binary operation makes $\mathbb{Z}/N$ into a commutative monoid with identity element 1.

   (b) Show that $(\mathbb{Z}/N)^\times$ is an abelian group.

   (c) Show that $(\mathbb{Z}/N)^\times$ consists of elements of $\mathbb{Z}/N$ which are relatively prime to N.

- (a) Unital: Fix $b = 1$. Then for $a \in \mathbb{Z}/N$,

  $$ab = a = 0N + a \equiv a \mod N.$$

  Commutative: Let $a, b \in \mathbb{Z}/N$. Then

  $$r \mod N \equiv qN + r = ab = ba = qN + r \equiv r \mod N.$$

  Associative: Let $a, b, c \in \mathbb{Z}/N$. From the division algorithm, $r_1, r_2, r_3, r_4, q_1, q_2, q_3, q_4 \in \mathbb{Z}$ such that

  $$\begin{aligned} ab &= q_1 N + r_1 \\ r_1 c &= q_2 N + r_2 \\ bc &= q_3 N + r_3 \\ a r_3 &= q_4 N + r_4 \end{aligned}$$

  We can then calculate $(a \cdot_N b) \cdot_N c = r_2$, and

  $$(ab - q_1 N)c = q_2 N + r_2 \Rightarrow abc - (q_1 c - q_2)N = r_2.$$

  Similarly, we have $a \cdot_N (b \cdot_N c) = r_4$, and

  $$abc - (q_3 a + q_4)N = r_4.$$

  Hence $r_4 \mod N \equiv abc \equiv r_2 \mod N$, as desired.

(b) Associativity and commutativity follow from (a) and the fact that $(\mathbb{Z}/N)^\times \subseteq \mathbb{Z}/N$. Note that $1 \cdot 1 \equiv 1 \mod N$, so $1 \in (\mathbb{Z}/N)^\times$. Now, let $a \in (\mathbb{Z}/N)^\times$. There exists some $b \in \mathbb{Z}/N$ such that

$$ab = ba = 1,$$

so $b \in (\mathbb{Z}/N)^\times$ and thus $b = a^{-1} \in (\mathbb{Z}/N)^\times$. Finally, let $a, b \in (\mathbb{Z}/N)^\times$. The existence of inverses implies that $b^{-1} \cdot_N a^{-1} = (a \cdot b)^{-1} \in \mathbb{Z}/N$, and by associativity,

$$\begin{aligned}(a \cdot_N b) \cdot_N (b^{-1} \cdot_N a^{-1}) &= a \cdot_N (b \cdot_N b^{-1}) \cdot_N a^{-1} \\ &= a \cdot_N a^{-1} \\ &= 1\end{aligned}$$

(c) Let $a \in \mathbb{Z}/N$. Suppose $\gcd(a, N) = c > 1$ and that there exists some b such that $ab \cong 1 \mod N$. Then

$$\begin{aligned}0 &\equiv \frac{a}{c} Nb \\ &\equiv ab\frac{N}{c} \\ &\equiv 1\frac{N}{c} \\ &\not\equiv 0 \mod N,\end{aligned}$$

a contradiction. Now, suppose $gcd(a, N) = 1$, and consider the set $S = \{0, a \mod N, \ldots, (N-1)a \mod N\}$. Since a and N are coprime, it follows from Bezout that $1 \in S$. Thus $a \in (\mathbb{Z}/N)^\times$.

□

2 9/27

1. Justify Example 4.7. Fix pairwise commuting elements $f_1, \ldots, f_r$ of a group G, i.e. elements such that $f_i f_j = f_j f_i$ for all $1 \leq i, j \leq r$. Prove that if each f_i has finite order n_i, then $f = f_1 \cdots f_r$ has order dividing the least common multiple of $f_1, \ldots, f_r$. Show that if moreover $f_1, \ldots, f_r$ are pairwise disjoint cycles in a symmetric group S_n, then the order of $f = f_1 \cdots f_r$ is exactly the least common multiple of $f_1, \ldots, f_r$.

   - Let $f = f_1 \cdots f_r$, where the f_i's pairwise commute. It directly follows (with an induction argument) that $f^m = f_1^m \cdots f_r^m$ for $m \in \mathbb{N}$. Denote the order of each f_i by n_i, the order of f by a, and define $n = \mathrm{lcm}_i\{n_i\}$. Note that

$$\begin{aligned}f^a &= f_1^a \cdots f_r^a \\ &= (f_1^{n_1})^{\frac{n}{n_1}} \cdots (f_r^{n_r})^{\frac{n}{n_r}} \\ &= e^{\frac{n}{n_1}} \cdots e^{\frac{n}{n_r}} \\ &= e.\end{aligned}$$

Clearly, if a divides n, we're done. Suppose otherwise; thus, $n < a$ since $f^a = e$. But, by the Euclidean division algorithm,

$$\begin{aligned} f^{n \mod a} &= f^n \cdot (f^{pa})^{-1} \\ &= f^n \cdot e \\ &= e \end{aligned}$$

for some $p \in \mathbb{Z}$. Since $n \mod a < a$, the order $|f| < a$, a contradiction.

- Let $\{f_i\}$ be pairwise disjoint cycles in a symmetric group S_n, each with length k_i, and similarly notate $k = \mathrm{lcm}_i\{k_i\}$ and a to be the order of $f = f_1 \cdots f_r$. Suppose that $a \neq k$, or equivalently, that $a < k$. Thus, there exists an i such that k_i does not divide a, and thus an n such that $f_i^a(n) = n$. Since f_i are disjoint, they commute, and we have

$$\begin{aligned} f^a(n) &= (f_i^a \cdot f_1^a \cdots f_{i-1}^a \cdot f_{i+1}^a \cdots f_r^a)(n) \\ &= f_i^a(n) \\ &\neq n \end{aligned}$$

since a is not divisible by k_i. Thus, $f^a \neq e$, a contradiction. $\square$

2. By Lemma 4.5, every element $f \in S_n$ can be written as a product of transpositions. Suppose that $f = g_1 \circ \cdots \circ g_k$, where $g_1, \ldots, g_k$ are transpositions. We say that f is **even** if k is even and we say that f is **odd** if k is odd. Show that this is well-defined by proving that if $f = h_1 \circ \cdots \circ h_m$ is another way of writing f as a product of transpositions, then $k \equiv m \mod 2$.

   - Ran out of time :(I have a midterm at 9 am tomorrow morning so this question's going to be an L. A brief outline of what I had in mind is as follows: Define the sign of a permutation f to be the number of inversions modulo 2. The desired result follows from showing $f \circ (a_i\ a_j)$ changes the sign of f. Since e is even (with 0 inversions), f is odd if, and only if, the sign of f is odd. $\square$

3. Let $f = (\, a_1 \ \cdots \ a_k \,)$ be a cycle. Show that f is even if k is odd and that f is odd if k is even.

   - Note that $f = (\, a_1 \ \cdots \ a_k \,) = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{k-1}\ a_k)$ can be written as a product of $k-1$ transpositions. Thus if k is odd, then $k-1$, and so f, is even. Similarly, if k is even, then f is odd. $\square$

4. Write down the cycle decomposition of each element of S_4 and compute the order of each element.

   - See below. $\square$

$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$
$(1)(2)(3)(4)$	$(1)(2\ 3)(4)$	$(1)(2\ 4\ 3)$	$(1)(2\ 3\ 4)$	$(1)(2\ 4)(3)$	$(1)(2)(3\ 4)$
1	2	3	3	2	2
$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$
$(1\ 2)(3)(4)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)(4)$	$(1\ 2\ 3\ 4)$	$(1\ 2\ 4\ 3)$	$(1\ 2\ 4)(3)$
2	2	3	4	4	3
$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$
$(1\ 3\ 2)(4)$	$(1\ 3\ 4\ 2)$	$(1\ 3)(2)(4)$	$(1\ 3\ 4)(2)$	$(1\ 3)(2\ 4)$	$(1\ 3\ 2\ 4)$
3	4	2	3	2	4
$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$
$(1\ 4\ 3\ 2)$	$(1\ 4\ 2)(3)$	$(1\ 4)(3)(2)$	$(1\ 4\ 3)(2)$	$(1\ 4\ 2\ 3)$	$(1\ 4)(2\ 3)$
4	3	2	3	4	2

cycle sizes

* Note that $|f| = \operatorname{lcm}(\text{cycle sizes})$ for $f \in S_4$.

5. See Dummit-Foote, Exercise 1.3.2 for the definitions of f and g, two elements of S_{15}. Find cycle

decompositions for $f, g, f^2 f \circ g, g \circ f$, and $g^2 \circ f$.

- $f =$
$$(1\ 13\ 5\ 10) \circ (3\ 15\ 8) \circ (4\ 14\ 11\ 7\ 12\ 9)$$
$g =$
$$(1\ 14) \circ (2\ 9\ 15\ 13\ 4) \circ (3\ 10) \circ (5\ 12\ 7) \circ (8\ 11)$$
$f^2 =$
$$(1\ 5) \circ (3\ 8\ 15)\ (4\ 11\ 12) \circ (7\ 9\ 14) \circ (10\ 13)$$
$f \circ g =$
$$(1\ 11\ 3) \circ (2\ 4) \circ (5\ 9\ 8\ 7\ 10\ 15) \circ (13\ 14)$$
$g \circ f =$
$$(1\ 4) \circ (2\ 9) \circ (3\ 13\ 12\ 15\ 11\ 5) \circ (8\ 10\ 14)$$
$g^2 \circ f =$
$$(1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$$
$\square$

3 9/29

1. Prove that if $n \geq 3$, then S_n is not cyclic.

   - We will first show that $\mathbb{Z}/N$ is abelian for $N \in \mathbb{N}$. Let $N \in \mathbb{N}, x, y \in \mathbb{Z}/N$. It follows from commutativity of the usual binary operation in $(\mathbb{Z}, +)$ that
   $$x + y \equiv (x + y) \mod N = (y + x) \mod N \equiv y + x,$$
   as desired. Now, let $n \geq 3$. By Proposition 3.8, we have that S_n is not abelian. However, if S_n is cyclic, then $S_n \cong \mathbb{Z}/N$ for some $N \in \mathbb{N}$, which we've shown to be abelian, a contradiction. $\square$

2. Recall that group $(\mathbb{Z}/N)^\times$ from Exercise 3.4. Let $\phi(N)$ be the number of elements of $(\mathbb{Z}/N)^\times$. The function ϕ is called the **Euler totient function.**

   (a) Show that if $M, N \geq 1$ are relatively prime, then $\phi(MN) = \phi(M)\phi(N)$.
   (b) Show that if $n \geq 1$, then for every prime number p we have $\phi(p^n) = p^{n-1}\phi(p)$.
   (c) Show that $\phi(p) = p - 1$ if p is prime.
   (d) What is $\phi(3072)$?

   - (a) Let $M, N \geq 1$ be relatively prime. Recall from Problem 1.4c that $(\mathbb{Z}/N)^\times$ consists of elements of $\mathbb{Z}/N$ which are relatively prime to N. Thus $= \phi(MN)$ is the size of the set
   $$(\mathbb{Z}/N)^\times = \{x \in \mathbb{Z}/MN \mid x \text{ and } MN \text{ are relatively prime}\}.$$

– **Lemma 1**: x, MN are coprime $\iff$ x and M are coprime or x and N are coprime. *Proof:* ($\Rightarrow$) Without loss of generality, assume x, N are not coprime. Then there exists some prime p such that $p|x$ and $p|N$. Thus $p|MN$ as well. ($\Leftarrow$) Suppose there exists some prime p such that $p|x$ and $p|MN$. By Euclid, either $p|M$ or $p|N$.

– **Lemma 2**: a and b are coprime $\iff$ $a \mod b$ and b are coprime. *Proof:* This follows directly from Euclid's GCD algorithm.

Let's define the following system of equations

$$(\star) = \begin{cases} x \equiv m \mod M \\ x \equiv n \mod N \end{cases}, m \in (\mathbb{Z}/M)^\times, n \in (\mathbb{Z}/N)^\times$$

Thus, we have that

$$(\mathbb{Z}/N)^\times = \{x \in \mathbb{Z}/MN \mid x \text{ satisfies } (\star)\}.$$

Then, for each $m \in (\mathbb{Z}/M)^\times, n \in (\mathbb{Z}/N)^\times$, the Chinese Remainder Theorem gives a unique $a \in \{0, \ldots, MN-1\}$ satisfying $(\star)$. There are $\phi(M)$ such elements m and $\phi(N)$ such elements n, so

$$\phi(MN) = \phi(M)\phi(N).$$

(b) Let $n \geq 1$. Notice that $\phi(p^n)$ is the size of the set

$$(\mathbb{Z}/p^n)^\times = \{x \in \mathbb{Z}/p^n \mid x \text{ and } p^n \text{ are relatively prime.}\}$$

– **Lemma:** p^n and a are coprime $\iff$ p and a are coprime. *Proof:* ($\Rightarrow$) If $x|a$ and $x|p$, then $x|p^n$, so p^n and x are not coprime. ($\Leftarrow$) Suppose $x|p^n$. then the Fundamental Theorem of Algebra gives that $x = p$. If $x|a$, then $p|a$, a contradiction.

Thus, we have that

$$(\mathbb{Z}/p^n)^\times = \{x \in \mathbb{Z}/p^n \mid x \equiv p' \mod p, p' \in (\mathbb{Z}/p)^\times\}.$$

Then, for each $p' \in (\mathbb{Z}/p)^\times$, the Chinese Remainder Theorem gives a unique solution x up to p consecutive elements, i.e.

$$\phi(p^n) = \frac{p^n}{p}\phi(p) = p^{n-1}\phi(p).$$

(c) Let p be prime. Notice that $0|p$ and $p|p$ so $0 \notin (\mathbb{Z}/p)^\times$. If $1 \leq x < p$, then x and p are coprime since p is prime. Thus $(\mathbb{Z}/p)^\times = \{1, \ldots, p-1\}$ so $\phi(p) = p - 1$.

(d) Notice that $3072 = 3 \cdot 2^{10}$. Then

$$\begin{aligned} \phi(3072) &= \phi(3 \cdot 2^{10}) \\ &= \phi(3)\phi(2^{10}) && (a) \\ &= \phi(3) \cdot 2^9 \cdot \phi(2) && (b) \\ &= 2 \cdot 512 \cdot 1 && (c) \\ &= 1024 \end{aligned}$$

□

3. Let $f : X \to Y$ be a bijection. Consider the permutation groups S_X and S_Y and the function $g : S_X \to S_Y$ defined by $g(h) = f \circ h \circ f^{-1}$ for $h \in S_X$. Prove that g is a group isomorphism.

   - Let $h_1, h_2 \in S_X$. Then by the associativity of functions,

     $$\begin{aligned} g(h_1 \circ h_2) &= f \circ h_1 \circ h_2 \circ f^{-1} \\ &= f \circ h_1 \circ Id_{X \to X} \circ h_1 \circ f^{-1} \\ &= f \circ h_1 \circ (f^{-1} \circ f) \circ h_1 \circ f^{-1} \\ &= (f \circ h_1 \circ f^{-1}) \circ (f \circ h_1 \circ f^{-1}) \\ &= g(h_1) \circ g(h_2) \end{aligned}$$

     so g is a homomorphism. Moreover, each element of S_X is a bijection, so if $h \in S_X$, then $g(h) = f \circ h \circ f^{-1}$ is a composition of bijections, and thus also a bijection. □