We make a few notational changes to facilitate arithmetic:

- In any k-cycle, we "zero-index" the elements; that is, $(a_1 a_2 \dots a_k)$ becomes $(a_0 a_1 \dots a_{k-1})$.
- In any k-cycle, addition (and subtraction), unless indicated otherwise, signify modular arithmetic with respect to k (e.g. $a \pm b$ becomes $a \pm b \mod k$).
- Finally, for any cycle $\sigma = (a_i a_j \dots a_k)$, let $V_\sigma = \{a_i, a_j, \dots, a_k\}$, and let $V_n = \{1, 2, \dots, n\}$.

Problem §1

(a) Express the following as products of disjoint cycles:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 5 & 4 & 7 & 9 & 8 & 6 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 2 & 4 & 9 & 8 & 7 & 6 \end{pmatrix}.$$

(b) Prove that a k-cycle in $\mathcal{S}_n$ has order k.

(c) Prove that the inverse of $(a_0 a_1 \dots a_{k-1})$ in $\mathcal{S}_n$ is $(a_0 a_{k-1} a_{k-2} \dots a_2 a_1)$

(d) Prove that disjoint cycles commute.

Solution:

(a) σ and τ in cycle notation become

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 5 & 4 & 7 & 9 & 8 & 6 \end{pmatrix} = (12)(45)(679)$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 2 & 4 & 9 & 8 & 7 & 6 \end{pmatrix} = (13)(254)(69)(78).$$

(b) Let $\sigma = (a_0 a_1 \dots a_{k-1})$. By definition, every a_i is unique; thus, for any a_i,

$$\sigma^j(a_i) = a_{i+j},$$

and $a_{i+j} = a_i$ only when $i + j \mod k \equiv i$. Clearly, $j = k$ is the smallest positive integer which satisfies that; thus

$$\sigma^k(a_i) = a_{i+k} = a_i,$$

and a_i has "order" k (that is, applying σ k times to a_i yields a_i). Since every element $a_i \in V_n$ has "order" k, k is the smallest positive integer such that $\sigma^k = e$, and so σ has order k.

(c) Let $\sigma = (a_0 a_1 \dots a_{k-1})$, where $\sigma(a_i) = a_{i+1}$ for any $a_i \in V_\sigma$.

Define $\tau(a_i) = a_{i-1}$, where $V_\tau = V_\sigma$ (that is, σ and τ operate on the same subset of V_n). Then τ in cycle notation is

$$\tau = (a_0 a_{k-1} a_{k-2} \dots a_2 a_1).$$

For any $a_i \in V_\sigma$, we have

$$\sigma \circ \tau(a_i) = \sigma(a_{i-1}) = a_{i-1+1} = a_i$$
$$\tau \circ \sigma(a_i) = \tau(a_{i+1}) = a_{i+1-1} = a_i.$$

Thus $\tau = (a_0 a_{k-1} \dots a_2 a_1) = \sigma^{-1}$ is the inverse of σ.

(d) Let $\sigma = (a_0 a_1 \dots a_{k-1})$ and $\tau = (b_0 b_1 \dots b_{r-1})$ be disjoint cycles; that is, $V_\sigma \subseteq V_n$, $V_\tau \subseteq V_n$, and $V_\sigma \cap V_\tau = \varnothing$. Moreover, by definition of a cycle π, if $\alpha \notin V_\pi$, then $\pi(\alpha) = \alpha$.

Let $\alpha \in V_n$. There are three possibilities:

- α is not in either V_σ or V_τ.
  Trivially, $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha) = \alpha$, by definition of a cycle.
- α is in V_σ, but not V_τ.
  If $\alpha \in V_\sigma$, then $\alpha = a_i$ for some $a_i \in V_\sigma$, and so $\sigma(\alpha) = a_{i+1}$. But for any $a \in V_\sigma$, $a \notin V_\tau$; thus $\tau(a) = a$. Hence
  $$\sigma \circ \tau(\alpha) = \sigma(\alpha) = a_{i+1} = \sigma(\alpha) = \tau \circ \sigma(\alpha),$$
  and so $\sigma\tau = \tau\sigma$, as required.
- α is in V_τ, but not V_σ.
  A similar structure follows. $\alpha \in V_\tau$ implies $\alpha = b_i$ for some $b_i \in V_\tau$, and so $\tau(\alpha) = b_{i+1}$. Additionally, $\sigma(b) = b$ for any $b \notin V_\sigma$, and so
  $$\tau \circ \sigma(\alpha) = \tau(\alpha) = b_{i+1} = \tau(\alpha) = \sigma \circ \tau(\alpha).$$

Since $V_\sigma \cap V_\tau = \varnothing$, α cannot be in both V_σ and V_τ. Therefore, if σ and τ are disjoint cycles, then for any $\alpha \in V_n$, $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha)$, and so
$$\sigma\tau = \tau\sigma.$$

Problem §2 Prove that every permutation in S_n can be written as a product of disjoint cycles.

Solution: Let π be any permutation in S_n. We make two observations:

- Since V_n is finite and π bijective, for any $\alpha \in V_n$, repeatedly applying $\pi(\alpha)$ (e.g. k times) will eventually yield α. Moreover, $k \leq n$, since otherwise we would get more than n distinct elements, a contradiction of V_n having only n elements.
- Any $\pi^i(\alpha)$ for $0 \leq i < k$ is unique; if we have $\pi^i(\alpha) = \pi^j(\alpha)$, where $0 \leq i \leq j < k$, we necessarily have $i = j$ (since $\alpha = \pi^{j-i}(\alpha)$, so $j - i = 0$).

Let $a \in V_n$, and let $\pi^i(a) = a_i$ with $\pi^k(a) = a$. Then $a_0, a_1, \ldots, a_{k-1}$ form a cycle
$$\sigma_a = (a_0 a_1 \ldots a_{k-1}),$$
since $a_k = a$ and all a_i are unique (from the observations).

Choose $b \in V_n \setminus V_{\sigma_a}$; that is, any $b \in V_n$ not in the cycle σ_a. Similarly, with $\pi^i(b) = b_i$ and $\pi^r(b) = b$, $b_0, \ldots, b_{r-1}$ form a cycle
$$\sigma_b = (b_0 b_1 \ldots b_{r-1}).$$
Crucially, $V_{\sigma_a} \cap V_{\sigma_b} = \varnothing$ (i.e. they share no elements); otherwise, if $b_i = a_j$ for some i, j, then any $b_i \in V_{\sigma_b}$ could be rewritten as $\pi^{j+t}(a)$ for some $t \in \mathbb{Z}$, a contradiction of $b \notin V_{\sigma_a}$.

Repeating this step until $V = V_{\sigma_a} \cap V_{\sigma_b} \cap \ldots \cap V_{\sigma_m}$, we see that π can be written as a product of disjoint cycles $\sigma_a, \sigma_b, \ldots, \sigma_m$.

Problem §3

(a) Show that the following formulae are true:
$$(a_0 a_1 \ldots a_{k-1}) = (a_0 a_{k-1})(a_0 a_{k-2}) \ldots (a_0 a_2)(a_0 a_1) = (a_0 a_1)(a_1 a_2) \ldots (a_{k-2} a_{k-1}).$$

(b) Prove that every permutation in S_n can be written as a product of transpositions.

(c) Express
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 2 & 4 & 6 & 8 & 9 & 7 \end{pmatrix}$$
as a product of transpositions.

Solution:

(a) Let $\sigma = (a_0 \dots a_{k-1})$, where $\sigma(a_i) = a_{i+1}$.

Let $\sigma^{(j)} = (a_0 a_j a_{j+1} \dots a_{k-1})$ for some $0 < j < k$. Suppose τ_i is some transposition where $\tau_i = (a_0 a_i)$. Then for $i = 1$, $\sigma = \sigma^{(1)}$ can be rewritten as

$$\sigma^{(1)} = (a_0 a_2 \dots a_{k-1})(a_0 a_1) = \sigma^{(2)} \tau_1.$$

One can quickly verify that this equality holds. Instead of directly mapping $a_1 \mapsto a_2$, we simply "reroute" it to a_0 : $a_1 \mapsto a_0 \mapsto a_2$; all other elements are unaffected.

Similarly, $\sigma^{(2)}$ can be rewritten as

$$\sigma^{(2)} = (a_0 a_3, , , a_{k-1})(a_0 a_2) = \sigma^{(3)} \tau_2,$$

and so $\sigma^{(1)} = \sigma$ becomes

$$(a_0 a_3 ... a_{k-1})(a_0 a_2)(a_0 a_1).$$

Repeating this process until $\sigma^{(k-1)}$, we get

$$\sigma = (a_0 a_1 \dots a_{k-1}) = (a_0 a_{k-1})(a_0 a_{k-2}) \dots (a_0 a_2)(a_0 a_1).$$

Now, let $\sigma_{(m)} = (a_0 a_1 \dots a_{m-1} a_m)$ for $0 < m < k$, and suppose τ_i now represents the transposition $a_i a_{i+1}$. Then for $m = k-1$, $\sigma = \sigma_{(k-1)}$ can be rewritten as

$$\sigma_{(k-1)} = (a_0 a_1 \dots a_{k-2})(a_{k-2} a_{k-1}) = a_{(k-2)} \tau_{k-2}.$$

Like before, verifying equality is simple; all of $a_0, \dots, a_{k-2}$ are unaffected, and a_{k-1} takes the scenic route of $a_{k-1} \mapsto a_{k-2} \mapsto a_0$, rather than simply $a_{k-1} \mapsto a_0$.

Similarly, $\sigma_{(k-2)}$ can be rewritten as

$$\sigma_{(k-2)} = (a_0 a_1 \dots a_{k-3})(a_{k-3} a_{k-2}) = \sigma_{(k-3)} \tau_{k-3},$$

and so $\sigma_{(k-1)} = \sigma$ becomes

$$(a_0 a_1 \dots a_{k-3})(a_{k-3} a_{k-2})(a_{k-2} a_{k-1}).$$

Repeating this process until $\sigma_{(1)}$, we get

$$\sigma = (a_0 a_1 \dots a_{k-1}) = (a_0 a_1)(a_1 a_2) \dots (a_{k-2} a_{k-1}).$$

Thus

$$(a_0 a_1 \dots a_{k-1}) = (a_0 a_{k-1})(a_0 a_{k-2}) \dots (a_0 a_2)(a_0 a_1) = (a_0 a_1)(a_1 a_2) \dots (a_{k-2} a_{k-1}).$$

(b) From Problem 2, we know that any permutation $\pi \in \mathcal{S}_n$ can be expressed as a product of disjoint cycles $\sigma_1, \sigma_2, \dots, \sigma_k$:

$$\pi = \sigma_1 \sigma_2 \dots \sigma_k.$$

Moreover, Problem 3a showed that any cycle σ can be expressed as a product of transpositions $\tau_1, \tau_2, \dots, \tau_m$:

$$\sigma = \tau_1 \tau_2 \dots \tau_m.$$

Rewriting every disjoint cycle as a product of transpositions, (since composition is associative, a product of product of transpositions becomes just a product of transpositions) we get that any permutation $\pi \in \mathcal{S}_n$ can be written as a product of transpositions.

(c)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 2 & 4 & 6 & 8 & 9 & 7 \end{pmatrix} = (13)(254)(789) = (13)(25)(54)(78)(89).$$

Problem §4

(a) If τ is a transposition in $\mathcal{S}_n$, and $\sigma \in \mathcal{S}_n$, prove that $\sigma\tau\sigma^{-1}$ is a transposition.

(b) More generally, if τ is the k-cycle $(a_0 a_1 \dots a_{k-1})$ and if $\sigma \in \mathcal{S}_n$, then $\sigma\tau\sigma^{-1} = (\sigma(a_0)\sigma(a_1)\dots\sigma(a_{k-1}))$.

Solution: Since σ is a bijection, any element $\alpha \in V_n$ can be expressed as $\sigma(a) \in V_n$ for some distinct $a \in V_n$. Thus, choose any $\sigma(a_i) \in V_n$, where $a_i \in V_\tau$. Then

$$\sigma \circ \tau \circ \sigma^{-1}(\sigma(a_i)) = \sigma \circ \tau(a_i) = \sigma(a_{i+1}),$$

and so any $\sigma(a_i)$ with $a_i \in V_\tau$ is mapped to $\sigma(a_{i+1})$ (for $i = k-1$, recall modular arithmetic: $a_{i+1} = a_k = a_0$). Thus, $\sigma\tau\sigma^{-1}$ forms a cycle $(\sigma(a_0)\sigma(a_1)\dots\sigma(a_{k-1}))$.

To show equality (that is, $\sigma\tau\sigma^{-1}$ is comprised of no other cycles), consider everything else; that is, any $\sigma(b) \in V_n$ where $b \notin V_\tau$. Since $\tau(b) = b$, we have

$$\sigma \circ \tau \circ \sigma^{-1}(\sigma(b)) = \sigma \circ \tau(b) = \sigma(b).$$

In other words, any $\sigma(b) \in V_n$ where $b \notin V_\tau$ "vanishes" in cycle notation.

Therefore, if $\tau = (a_0 a_1 \dots a_{k-1})$ and $\sigma \in \mathcal{S}_n$, then $\sigma\tau\sigma^{-1} = (\sigma(a_0)\sigma(a_1)\dots\sigma(a_{k-1}))$ [which proves part b].

Setting $k = 2$, we see that $\sigma\tau\sigma^{-1} = (\sigma(a_0)\sigma(a_1))$, and so τ transposition implies $\sigma\tau\sigma^{-1}$ transposition as well [which proves part a].

Problem §5

(a) If G is a group with order 25, prove that G is cyclic or else every non-identity element in G has order 5. Do you think this argument can generalize? If so, explain how; if not, explain why you think so.

(b) Let a be an element with order 30 in a group G; what is the index of $\langle a^4 \rangle$ in the group $\langle a \rangle$?

Solution:

(a) Let G be a group with order 25. G can clearly be cyclic:

$$G = \{g^1, g^2, \dots, g^{24}, g^{25} = e\};$$

so suppose G is not cyclic.

Let $g \in G$ be a non-identity element. g cannot have order 25 (since otherwise G would be cyclic, a contradiction), so suppose $|g| = k$ for some $1 < k < 25$. Then the cyclic subgroup

$$\langle g \rangle = \{g^1, g^2, \dots, g^k = e\} < G.$$

has order k. By Lagrange's Theorem, any subgroup's order divides the order of G; but since 25 only has divisors $1, 5$, and 25, and $1 < k < 25$, k must necessarily be 5. Thus if G is not cyclic, any non-identity element $g \in G$ has order 5.

A natural generalization would be:

If G has order a^2, then G is either cyclic or every non-identity element $g \in G$ has order a.

However, this is clearly not true for something like $a = 4$; $\mathcal{D}_8$, for instance, has non-identity elements with order 2 (e.g. flips).

Thus, a stricter generalization is necessary:

If p is a prime number, and a group G has order p^2, then G is either cyclic or every non-identity element $g \in G$ has order p.

This seems to be true; replacing 5 with p and 25 with p^2 in the above proof seems to maintain sound logic without problem.

(b) Since the order of a is 30, any $a^k = e$ must satisfy $k|30$ (by Corollary 2.42) or $a = 30n$ for some $n \in \mathbb{Z}$ (by Proposition 2.9). Since none of $4, 8, \ldots, 56$ satisfy these conditions, the first multiple of 4 that satisfies these conditions is 60. Since $\frac{60}{4} = 15$, we have that $|\langle a^4 \rangle| = 15$. Since any a^i where $i > 30$ can be rewritten as $a^{30}a^{i-30} = e \cdot a^{30+2+4j-30} = a^{4j+2}$, and a^i where $i < 30$ produces a^{4j}, $\langle a^4 \rangle$ is actually isomorphic to $\langle a^2 \rangle$ (since $\langle a^4 \rangle$ contains all multiples of 2 until 30). Since only 2 distinct cosets can be formed from $\langle a^2 \rangle$ ($e \langle a^2 \rangle$ and $a \langle a^2 \rangle$; any $a^{2k+i} \langle a^2 \rangle$ will end up forming the same coset), we have that

$$(\langle a \rangle : \langle a^2 \rangle) = (\langle a \rangle : \langle a^4 \rangle) = 2,$$

or equivalently, $\langle a^4 \rangle$ has index 2 in the group $\langle a \rangle$.

Problem §6

(a) Let $f : G \to H$ be a homomorphism of groups and let $a \in G$. Prove that if $a \in G$ has finite order, then $f(a)$ has finite order and $|f(a)|$ divides $|a|$.

(b) What condition(s) could you impose on f that would allow you to replace "divides" by "is equal to" above?

Solution:

(a) Suppose G, H are groups and $f : G \to H$ is a homomorphism, and suppose an $a \in G$ has finite order k. Then

$$\begin{aligned} f(a^k) &= f(\underbrace{a \cdot \ldots \cdot a}_{k \text{ times}}) \\ f(e) &= \underbrace{f(a) \cdot \ldots \cdot f(a)}_{k \text{ times}} \\ e' &= f^k(a). \end{aligned}$$

By Proposition 2.9, k divides the order of $f(a)$; in other words, $k = n\,|f(a)|$ for some $n \in \mathbb{Z}$. Hence $f(a)$ has finite order as well; and since k is the order of a, the order of $f(a)$ divides a.

(b) The primary condition to impose on f would be isomorphism:

If $f : G \to H$ is an isomorphism and $a \in G$ has order k, then $f(a) \in H$ has order k as well.

Proof. From above, we see that the order of $f(a)$ divides k. Let n denote the order of $f(a)$, and suppose $n < k$. Then

$$\begin{aligned} f(a^{n+1}) &= f^{n+1}(a) \\ &= f^n(a) \cdot f(a) \\ &= e' \cdot f(a). \end{aligned}$$

But this contradicts injectivity, since $f(a^{n+1}) = f(a^1) = f(a)$. Thus $n = k$, and so the order of $f(a)$ equals the order of a. □

From this, though, it seems that we can be slightly looser with our requirements; since only injectivity played a part, we need only require that

If $f : G \to H$ is an injective homomorphism and $a \in G$ has order k, then $f(a) \in H$ has order k as well.

The above proof also works for this statement.

However, surjective homomorphisms clearly do not necessarily preserve the order of an element; consider the identity homomorphism

$$\begin{aligned} f : G &\longrightarrow H \\ g &\longmapsto f(g) = e'. \end{aligned}$$

Clearly, the order of any $f(g) \in H$ is 1, while the order of any $g \in G$ is not necessarily 1.