§2.3 Permutations

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review

- (a, b) & $[a, b]$ $\dashrightarrow$ $(a, b) \cdot [a, b] = ab$
- $(a, b) | (am + bn)$, linear combination of a and b
- Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (matrix form)
- $(a, b) = 1 \Leftrightarrow am + bn = 1$ for some $m, n \in \mathbf{Z}$
- If $b|ac$ and $(a, b) = 1 \Rightarrow b|c$
- $a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow a = b + qn \Leftrightarrow [a]_n = [b]_n$
- If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$ (i.e., $a \in \mathbf{Z}_n^\times$) $\Rightarrow c \equiv d \pmod{n}$
- Divisor of zero **v.s.** Unit (Cancellation law ✓) in $\mathbf{Z}_n$
- Linear congruence $ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow (a, n)|b$
- System of congruences: Chinese Remainder Theorem
- For $[a] \in \mathbf{Z}_n^\times$, find $[a]^{-1}$:

  (i) the Euclidean algorithm (ii) successive powers (iii) trial and error
- Euler's totient function $\varphi(n) = \#\{a\colon (a, n) = 1, 1 \le a \le n\} = \#|\mathbf{Z}_n^\times|$
- Euler's theorem $\dashrightarrow$ Fermat's "little" theorem

Permutations

Let S be a set. A function $\sigma : S \to S$ is called a **permutation** of S if σ is one-to-one and onto. Denote $\mathrm{Sym}(S)$ by the set of all permutations of S.

The set of all permutations of the set $\{1, 2, \ldots, n\}$ will be denoted by S_n.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \in S_n$$

We write the image $\sigma(i)$ of i under each integer i. For example,
If $S = \{1, 2, 3\}$ and $\sigma : S \to S$ is given by $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$, so

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3.$$

S_n has $n!$ elements.

Proof: $\sigma(1)$: there are n choices; $\sigma(2)$: there are $(n-1)$ choices; [Why?]
$\sigma(3)$: there are $(n-2)$ choices; etc. $|S_n| = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = n!$. □

i). If $\sigma, \tau \in \mathrm{Sym}(S)$, then $\tau\sigma \in \mathrm{Sym}(S)$; ii). $1_S \in \mathrm{Sym}(S)$;
iii). If $\sigma \in \mathrm{Sym}(S)$, then $\sigma^{-1} \in \mathrm{Sym}(S)$.

Composition and Inverse in S_n

$\sigma, \tau \in S_n$: The **composition** $\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$.

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Compute $\sigma\tau$ and $\tau\sigma$.

$\sigma\tau(1) : 1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3 \Rightarrow \sigma\tau(1) = 3$, etc. We obtain $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$.

$\tau\sigma(1) : 1 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 1 \Rightarrow \sigma\tau(1) = 1$, etc. We obtain $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Given $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ in S_n, to compute σ^{-1}:

Key idea: If $\sigma(i) = j$, then $i = \sigma^{-1}(j)$.
i.e., turning the two rows of σ upside down and then rearranging terms.

If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, then $\sigma^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$.

Cycle

Another Notation

For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \in S_5$. We write $\sigma = (1342)$.
Observe that $\sigma(1) = 3,\ \sigma(3) = 4,\ \sigma(4) = 2$, and $\sigma(2) = 1$.
In the new notation we do not need to mention $\sigma(5)$ since $\sigma(5) = 5$.

Let S be a set, and let $\sigma \in \mathrm{Sym}(S)$. Then σ is called a **cycle of length** k if there exist elements $a_1, a_2, \ldots, a_k \in S$ such that

- $\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \ldots,\ \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1$, and
- $\sigma(x) = x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, \ldots, k$.

In this case we write $\sigma = (a_1 a_2 \cdots a_k)$.

We can also write $\sigma = (a_2 a_3 \cdots a_k a_1)$ or $\sigma = (a_3 a_4 \cdots a_k a_1 a_2)$, etc.
A cycle of length $k \geq 2$ can thus be written in k different ways, depending on the starting point.

We will use (1) to denote the identity permutation 1_S.

Examples

Example 1

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5, \text{ then } \sigma = (134) \text{ is a cycle of length } 3.$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5, \text{ then } \tau = (134)(25) \text{ is not a cycle.}$$

Example 2

Let $\sigma = (1425)$ *and* $\tau = (263)$ *be cycles in* S_6*. Compute the product* $\sigma\tau$*.*

$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 4 \Rightarrow \sigma\tau(1) = 4$, *etc.* $\Rightarrow \sigma\tau = (1425)(263) = (142635)$.

It is NOT true in general that the product of two cycles is again a cycle.

Example 3

Consider $(1425) \in S_6$, *we have* $(1425)(1425) = (12)(3)(45)(6) = (12)(45)$.

Disjoint Cycles

Let $\sigma = (a_1 a_2 \cdots a_k)$ and $\tau = (b_1 b_2 \cdots b_m)$ be cycles in $\mathrm{Sym}(S)$ for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

(12) and (45) are disjoint in S_6; but (1425) and (263) are not disjoint in S_6

If $\sigma\tau = \tau\sigma$, then we say that σ and τ **commute**.

In general, $\sigma\tau \neq \tau\sigma$. eg., In $S_3, (12)(13) = (132)$, but $(13)(12) = (123)$.

Let S be any set. If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Proof: Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_m)$ be disjoint.

If $i < k$, then $\sigma\tau(a_i) = \sigma(a_i) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(a_i)) = \tau\sigma(a_i)$.

If $i = k$, then $\sigma\tau(a_k) = \sigma(a_k) = a_1 = \tau(a_1) = \tau(\sigma(a_k)) = \tau\sigma(a_k)$.

If $j < m$, then $\sigma\tau(b_j) = \sigma(b_{j+1}) = b_{j+1} = \tau(b_j) = \tau(\sigma(b_j)) = \tau\sigma(b_j)$.

If $j = m$, then $\sigma\tau(b_m) = \sigma(b_1) = b_1 = \tau(b_m) = \tau(\sigma(b_m)) = \tau\sigma(b_m)$.

For any c not appearing in either cycle, we have $\sigma\tau(c) = c = \tau\sigma(c)$. $\square$

Product

Taking the composition of $\sigma \in \mathrm{Sym}(S)$ with itself i times is a permutation:

$$\sigma^i = \sigma\sigma\cdots\sigma.$$

Define $\sigma^0 := (1) = 1_S$ and $\sigma^{-n} := (\sigma^n)^{-1}$. For all integers m, n, we have

$$\sigma^m\sigma^n = \sigma^{m+n} \qquad \text{and} \qquad (\sigma^m)^n = \sigma^{mn}.$$

Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. And the cycles of length ≥ 2 that appear in the product are unique.

Proof: Consider $\sigma^0(1) = 1, \sigma(1), \sigma^2(1), \ldots$: since S has only n elements, we can find the least positive exponent r such that

$$\sigma^r(1) = 1.$$

Then $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ are all distinct, giving us a cycle of length r:

$$(1\ \sigma(1)\ \sigma^2(1)\ \cdots\ \sigma^{r-1}(1)). \qquad (\star)$$

If $r < n$, let a be the least integer not in $(\star)$ and form the cycle

$$(a\ \sigma(a)\ \sigma^2(a)\ \cdots\ \sigma^{s-1}(a))$$

in which s is the least positive integer such that $\sigma^s(a) = a$.

If $r + s < n$, we continue in this way until we have exhausted S. □

Examples

Every $\sigma \in S_n$ can be written as a unique product of disjoint cycles.

We actually give an algorithm in the proof for finding the necessary cycles.

Example 4

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 6 & 3 & 8 & 1 & 4 \end{pmatrix} = (1537)(468).$$

Example 5

Let $\sigma = (25143)$ *and* $\tau = (462)$ *be in* S_6. *Then we have* $\sigma\tau = (1465)(23)$.

Order of a Permutation

If $\sigma = (a_1 \cdots a_m)$ is a cycle of length m, then $\sigma^m(a_i) = a_i$ for $i = 1, \ldots, m$. Thus $\sigma^m = (1)$. And m is the smallest positive power of σ that equals (1).

The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

In particular, a cycle of length m has order m.

Let $\sigma \in S_n$ have order m. Then $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{m}$.

Proof: $(\Rightarrow)$ $\sigma^{i-j} = (1)$, write $i - j = mq + r$ with $0 \le r < m$. So

$$(1) = \sigma^{mq+r} = \left(\sigma^m\right)^q \sigma^r = \sigma^r \quad \Rightarrow r = 0. \text{ [Why?]}$$

$(\Leftarrow)$ Write $i = j + mk$ with $k \in \mathbf{Z}$. Hence $\sigma^i = \sigma^{j+mk} = \sigma^j$. □

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths (orders) of its disjoint cycles.

e.g., $(1537)(284)$ has order 12 in S_8; $(153)(284697)$ has order 6 in S_9.

Inverse Revisited

We merely reverse the order of the cycle to compute the inverse of a cycle:

$$(a_1 a_2 \cdots a_r)(a_r a_{r-1} \cdots a_1) = (1).$$

e.g., Let $\sigma = (1537) \in S_8$. Then $\sigma^{-1} = (7351) = (1735)$.

The inverse of the product $\sigma\tau$ of two permutations is $\tau^{-1}\sigma^{-1}$.

Proof: $(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma(1)\sigma^{-1} = \sigma\sigma^{-1} = (1)$. □

Thus for two cycles $(a_1 \cdots a_r)$ and $(b_1 \cdots b_m)$ we have

$$[(a_1 \cdots a_r)(b_1 \cdots b_m)]^{-1} = (b_m \cdots b_1)(a_r \cdots a_1).$$

Moreover, if these two cycles are disjoint, then they commute. And so

$$[(a_1 \cdots a_r)(b_1 \cdots b_m)]^{-1} = (b_m \cdots b_1)(a_r \cdots a_1) = (a_r \cdots a_1)(b_m \cdots b_1).$$

Example 6

$\sigma = (123), \tau = (456)$: $(\sigma\tau)^{-1} = (654)(321) = (321)(654) = (132)(465)$

Transposition

A cycle $(a_1 a_2)$ of length two is called a **transposition**.

Any $\sigma \in S_n$ $(n \geq 2)$ can be written as a product of transpositions.

Proof: Since any $\sigma \in S_n$ can be expressed as a product of disjoint cycles.

$\rightsquigarrow$ To show that any cycle can be expressed as a product of transpositions.

The identity $(1) = (12)(21)$. For any other $\sigma \neq (1)$, we have

$$\begin{aligned}(a_1 a_2 \cdots a_{r-1} a_r) =& (a_{r-1} a_r)(a_{r-2} a_r) \cdots (a_3 a_r)(a_2 a_r)(a_1 a_r) \quad (\star) \\ =& (a_1 a_2)(a_2 a_3) \cdots (a_{r-2} a_{r-1})(a_{r-1} a_r). \quad (\star\star)\end{aligned}$$

The way to write a product of transpositions is not unique. □

Example 7

$(25378) \overset{(\star)}{=} (78)(38)(58)(28) \overset{(\star\star)}{=} (25)(53)(37)(78).$

$(1) = (123) \cdot (132) \overset{(\star\star)}{=} (12)(23) \cdot (13)(32) \overset{(\star)}{=} (23)(13) \cdot (32)(12).$

Even/Odd Permutations

$(123) \overset{(\star)}{=} (23)(13) \overset{(\star\star)}{=} (12)(23)$, we also have $(123) = (12)(13)(12)(13)$.

If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even or odd in both cases.

Proof: See next slide. □

A permutation σ is called
even if it can be written as a product of an even number of transpositions.
odd if it can be written as a product of an odd number of transpositions.

For example, (12) and $(1234) \overset{(\star)}{=} (34)(24)(14) \overset{(\star\star)}{=} (12)(23)(34)$ are odd;
(123) and $(25378) \overset{(\star)}{=} (78)(38)(58)(28) \overset{(\star\star)}{=} (25)(53)(37)(78)$ are even;
The identity (1) is even since $(1) = (12)(21)$.

A cycle of odd length is even. & A cycle of even length is odd.

If σ is an even (resp. odd) permutation, then σ^{-1} is also even (resp. odd).

Proof of "$\sigma \in S_n$ is either even or odd"

Proof by contradiction: Suppose that σ can be both even and odd, i.e.,

$$\sigma = \tau_1 \cdots \tau_{2m} = \delta_1 \cdots \delta_{2n+1}, \qquad \tau_i, \delta_j \text{ are transpositions.}$$

Observe that $\delta_j = \delta_j^{-1}$, we have $\sigma^{-1} = \delta_{2n+1}^{-1} \cdots \delta_1^{-1} = \delta_{2n+1} \cdots \delta_1$, and so

$$(1) = \sigma\sigma^{-1} = \tau_1 \cdots \tau_{2m}\, \delta_{2n+1} \cdots \delta_1. \quad \Rightarrow (1) \text{ is odd.}$$

Assume $(1) = \rho_1 \cdots \rho_k$ $(k \geq 3)$ has the *shortest* product of transpositions.

Assume $\rho_1 = (ab)$. Then a must appear in at least one other transposition, say ρ_i, with $i > 1$. Otherwise, $\rho_1 \cdots \rho_k(a) = a = b$, which is impossible.

Among all products of length k that are equal to (1), and $\rho_1 = (ab)$, we assume that $\rho_1 \cdots \rho_k$ has the fewest number of a's.

Let a, u, v, w be distinct: $(uv)(aw) = (aw)(uv)$ and $(uv)(av) = (au)(uv)$.

Thus we can move a transposition with entry a to the 2nd position without changing the number of a's that appear. Say $\rho_2 = (ac)$ with $c \neq a$.

If $c = b$, then $\rho_1\rho_2 = (1)$, and so $(1) = \rho_3 \cdots \rho_k$. *(contradiction)*

If $c \neq b$, $(ab)(ac) = (ac)(bc) \Rightarrow (1) = (ac)(bc)\rho_3 \cdots \rho_k$. *(contradiction)*