

1/22

- last quiz on operations. Please let me know if you are still struggling on this topic.
- moving forward we will assume that we are a group.

Review Let $f: A \rightarrow B$. ↙ "f be a function from A to B"

Def 8. a) f is said to be injective (or one-to-one, or 1-1)
if $\forall a_1, a_2 \in A, (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$.

b) f is said to be surjective (or onto)
if $\forall b \in B \exists a \in A, f(a) = b$.

(f is inj. iff ~~if $f(a_1) = f(a_2)$, then $a_1 = a_2$~~
if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$ "horizontal line test")
f sur, iff $B = \text{range}(f)$)

c) if f is • injective & surjective, then f is bijective ^{called}
(or a "one-to-one correspondence".)

Def 9 A bijection from A onto itself is called
a permutation.

2

Let A be a set.

$$A^A$$

$$\mathcal{F}(A, B) = B^A$$

We denote $\mathcal{F}(A, A)$ the set of all function from A to A .

We define an operation on $\mathcal{F}(A, A)$ (called composition)

as for $f, g \in \mathcal{F}(A, A)$ $f \circ g$ is the function defined

by : for each $a \in A$ (A as the domain)

$$(f \circ g)(a) = f(g(a)).$$

this makes sense as $a \in A$
 $\Rightarrow g(a) \in A$ and so
 $f(g(a)) \in A$.

I. $\circ$ is associative : Let $f, g, h \in \mathcal{F}(A, A)$

We show that $(f \circ g) \circ h = f \circ (g \circ h)$.

$$\begin{aligned} f(x) &= x^2 \\ g(x) &= \sin x \\ (f \circ g)(x) &= f(\sin x) = (\sin x)^2 = \sin^2 x \end{aligned}$$

Recall to show that two functions are equal we show that they agree for all $a \in A$.

$$\begin{aligned} ((f \circ g) \circ h)(a) &= (f \circ g)(h(a)) = f(g(h(a))) \\ &\quad \text{def. of comp. applied to } f \circ g, h \\ &\quad \text{def. of comp. applied to } f, g. \end{aligned}$$

$$\begin{aligned} (f \circ (g \circ h))(a) &= f((g \circ h)(a)) = f(g(h(a))) \\ &\quad \text{def comp. app to } f, (g \circ h) \\ &\quad \text{def. of comp. applied to } g, h. \end{aligned}$$

So $\circ$ is associative.

II. ~~also~~ $\exists$ a $\circ$ -identity. Define $i: A \rightarrow A$ by $i(a) = a$.

Then $i \in \mathcal{F}(A, A)$. We let $f \in \mathcal{F}(A, A)$ be arbitrary and show $f \circ i = f$

$$(f \circ i)(a) = f(i(a)) = f(a) \quad \checkmark \quad \text{red } (f \circ i)(a) = f(a) \quad \forall a \in A \text{ so } \uparrow$$

$$i \circ f = f$$

$$(i \circ f)(a) = i(f(a)) = f(a) \quad \checkmark$$

③

Proposition

$$(\tilde{F}(A, A), o, i)$$

$\tilde{F}(A, A)$ is a monoid.

constant function

$$\forall x \in A \quad f(x) = a.$$

Ex. Let $A = \{a, b\}$. Define $f = \bar{a}$ (so $f(a) = f(b) = a$).
 $\in \tilde{F}(A, A)$.

We claim that $\nexists g \in \tilde{F}(A, A)$ s.t. $f \circ g = i$.

Pf. by contradiction: $\exists g \in \tilde{F}(A, A)$ and $f \circ g = i$.

$$\text{Then } (f \circ g)(b) = i(b) = b.$$

$$\text{But } f(g(b)) = a \text{ and } a \neq b.$$

This works for any set A as long as $|A| > 1$.

So in general $\tilde{F}(A, A)$ is not a group. (iff $|A| = 1$)

Def 10 Take the set of all permutations on A .

We denote this set by $\text{Perm}(A)$

$$(S(A), o) \quad o \equiv \text{composition}$$

zero
 $\downarrow$
 $0 \circ \text{comp}$
 f^{-1}

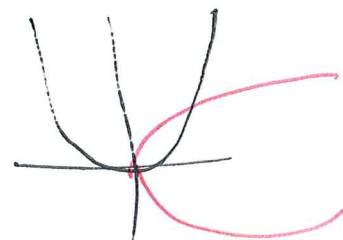
f be a perm. on A . Since f is inj it has an inverse function
 the $\text{dom}(f^{-1}) = \text{range}(f) = A$ onto

f^{-1} is a permutation

$$(f \circ f^{-1})(x) = x$$

$$= f(f^{-1}(x)) = x = i(x)$$

$$\forall x \in A \quad f^{-1} \circ f(x) = x = i(x)$$



4

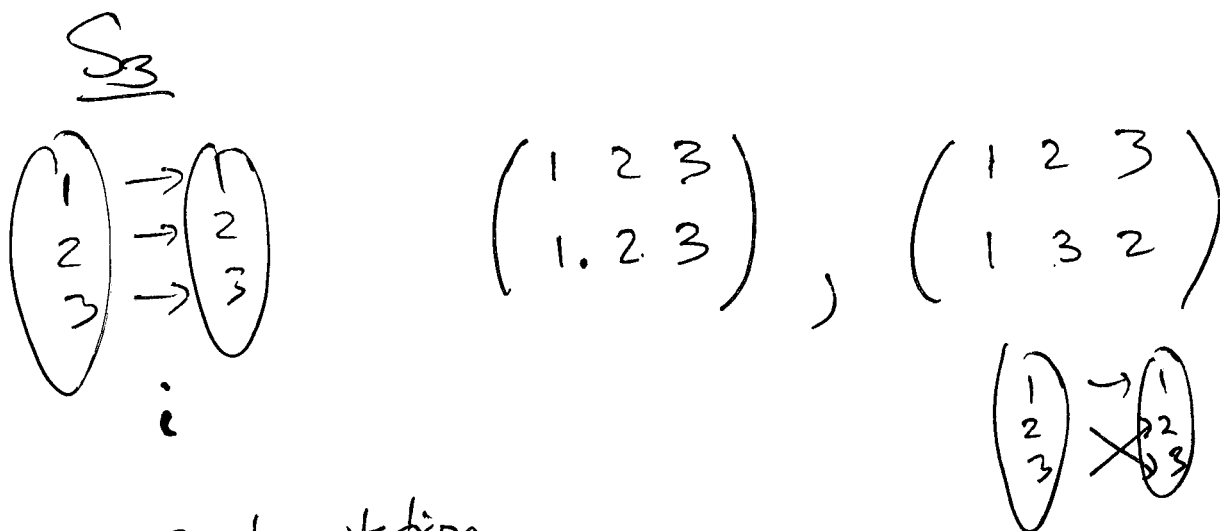
Thm $(S(A), \circ, i)$ is a group.

Notation when $A = \{1, \dots, n\}$ instead of $S(A)$
we write S_n

called the symmetric group on $\{1, \dots, n\}$

$(S_n, \circ, i)$ is a group

Question $|S_n| = \underline{n!}$



cycle notation

$(1)(23) \rightarrow (23)$

(123)

⑤ S_5

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$$

$f \in S_5$

$$f(3) = 4$$

$$f(2) = 2$$

$$f(4) = 5$$

$$f(1) = 3$$

$$f(5) = 1$$

$$(1345)(2) = \underline{(1345)}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

$$(132)(45) = (45)(132)$$

3,2-cycle

2,3-cycle

S_5

$$\sigma = (1234)$$

4-cycle.

$$\tau = (14)(25)$$

2,2 cycle.

$$(1234) = (2341) = (3412) \\ = (4123)$$

$$\neq \underline{(1243)}$$

⑥

$$\sigma = (1234), \tau = (14)(25)$$

right to left

$$\sigma \circ \tau = (1234)(14)(25)$$

$$1 \rightarrow 4 \rightarrow 1 \quad 1 \rightarrow 1$$

$$(1)(2534)$$

$$\phi \quad \sigma \circ \tau = (2534)$$

$$\sigma \circ \tau \neq \tau \circ \sigma$$

$$\tau \circ \sigma = (14)(25)(1234)$$

$$\tau \circ \sigma = (1523)$$

S_5 is not abelian

Cor S_n is abelian iff $n \leq 2$

$$(123)(12) = (13)$$

$$(12)(123) = (23)$$

~~S_3~~ not abelian

$(S_{3,0,i}) \uparrow$

$$|S_3| = 6.$$

In class we discussed the collection of functions from a fixed set S into the real numbers. The appropriate set-theoretic notation would be $\mathbb{R}^S$ but I have found that this notation is not so suggestive. So let's denote this set by $\mathcal{F}(S, \mathbb{R})$. Here the $\mathcal{F}$ can remind you of functions, and then S goes first since it is the domain, and then $\mathbb{R}$ since it is the co-domain.

In class we defined an operation on $\mathcal{F}(S, \mathbb{R})$ as follows: for $f, g \in \mathcal{F}(S, \mathbb{R})$, we defined $f \oplus g$ to be the function that sends each $s \in S$ to the real number $f(s) + g(s)$. We showed that the operation is associative and commutative. We also showed that there is a $\oplus$ -identity: the function $\bar{0}$ which sends everything in S to $0 \in \mathbb{R}$.

$$\bar{0} \oplus f = f.$$

We also showed that each function $f \in \mathcal{F}(S, \mathbb{R})$ has an $\oplus$ -inverse. It is the function that sends each $s \mapsto -f(s)$. Suggestively, we denote this function by $-f$. It follows that

$$f \oplus -f = \bar{0}.$$

Remark 0.1. The big idea in dealing with functions is that to show two functions $f, g \in \mathcal{F}(S, \mathbb{R})$ are equal, you have to show that **for all** $s \in S$, $f(s) = g(s)$.

Example 0.2. Let $T = \{0, 1\}$ and let $f, g, h \in \mathcal{F}(T, \mathbb{R})$ be defined by $f(t) = 2t+1$, $g(t) = 1+4t-2t^2$, and $h(t) = 5^t + 1$.

i) Show that $f = g$.

$$\begin{aligned} f(0) &= 2(0)+1 = 1 \\ g(0) &= 1+4(0)-2(0)^2 = 1 \\ f(1) &= 2(1)+1 = 3 \\ g(1) &= 1+4(1)-2(1)^2 = 3 \end{aligned} \quad \left| \quad (f \oplus g)(x) = f(x) + g(x) \right. \quad \text{so } f, g \text{ agree on all pts. in } T. \therefore f = g$$

ii) Show that $f \oplus g = h$.

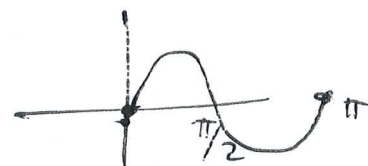
$$\begin{aligned} (f \oplus g)(0) &= f(0) + g(0) = 1 + 1 = 2 \\ h(0) &= 5^0 + 1 = 1 + 1 = 2 \\ (f \oplus g)(1) &= f(1) + g(1) = 3 + 3 = 6 \\ h(1) &= 5^1 + 1 = 5 + 1 = 6 \end{aligned} \quad \left| \quad \begin{aligned} (f \oplus g)(t) &= 3 + 3 = 6 \\ h(t) &= 5^t + 1 = 6 \end{aligned} \right. \quad \therefore f \oplus g = h$$

iii) Is f injective?

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 3 \end{aligned} \quad \left(\begin{array}{c} 0 \\ 1 \end{array} \right) \mapsto \left(\begin{array}{c} 1 \\ 3 \end{array} \right) \quad \text{injective.}$$

iv) Let $j \in \mathcal{F}(T, \mathbb{R})$ be defined by $j(t) = \sin(\pi t)$. True or False: $j = \bar{0}$.

$$\begin{aligned} j(0) &= 0 \\ j(1) &= 0 \end{aligned} \quad \text{so } j = \bar{0}$$



v) Is f surjective? If no, is there any $k \in \mathcal{F}(T, \mathbb{R})$ that is surjective.

$$\text{no \& no} \quad \text{b/c } T \text{ only has 2 pts.} \quad + \quad |k(t)| \leq 2 \leq |\mathbb{R}|$$

vi) If we take $T' = \{0, 1, 2\}$ are i), ii), iii) and iv) still true?

