Group Theory (Modern Algebra / Abstract Algebra)

<u>Def</u> A binary operation on a domain D is an operation / function mapping $D \times D$ to D. binary - arguments

e.g. $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ $\quad (+, \mathbb{N})$

$+ ; \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ $\quad (+, \mathbb{R})$

<u>closure</u>

<u>Def</u> A <u>structure</u> consists of an operation $\circ$ and a domain set D.

$\circ : D \times D \to D$ $\quad (\circ, D)$

A structure is associative if

$$\forall x \forall y \forall z \quad (x \circ y) \circ z = x \circ (y \circ z)$$

A structure that is associative is called a semigrap.

e.g. $(+, \mathbb{N}), (+, \mathbb{R}), (*, \mathbb{Z}), (\cancel{=},$

Non-examples ; $(-, \mathbb{N})$ is not a structure

$(-, \mathbb{Z})$ is a structure but not a semigroup.

Identity: $(\circ, D)$ has an <u>identity element</u> if

$$\exists i \in D \text{ s.t. } \forall x \in D \quad i \circ x = x \circ i = x$$

example: The identity element of $(+, \mathbb{Z})$ is 0

$(*, \mathbb{Z})$ is 1.

A semigroup with an identity element is called a <u>monoid.</u>

Inverses: $(\circ, D)$ has inverse if it has an identity and

$$\forall x \in D \ \exists x^{-1} \text{ s.t. } x \circ x^{-1} = x^{-1} \circ x = i$$

Example: The inverse of x in $(+, \mathbb{Z})$ is $-x$

A monoid with an inverse is called a group.

$(*, \mathbb{Z})$ is a monoid but not a group because 0 has no inverse

$(*, \mathbb{R})$

$(*, \mathbb{R} - \{0\})$ is a group. $\frac{1}{x}$

A structure is called "abelian"

if it is commutative.

Theorem: A monoid has exactly one identity element.

Assume i_1, i_2

$$i_2 = i_1 \circ i_2 = i_1$$

Theorem: A group has the property left-cancellation.

If $z \circ x = z \circ y$ then $x = y$

Proof: $z \circ x = z \circ y$

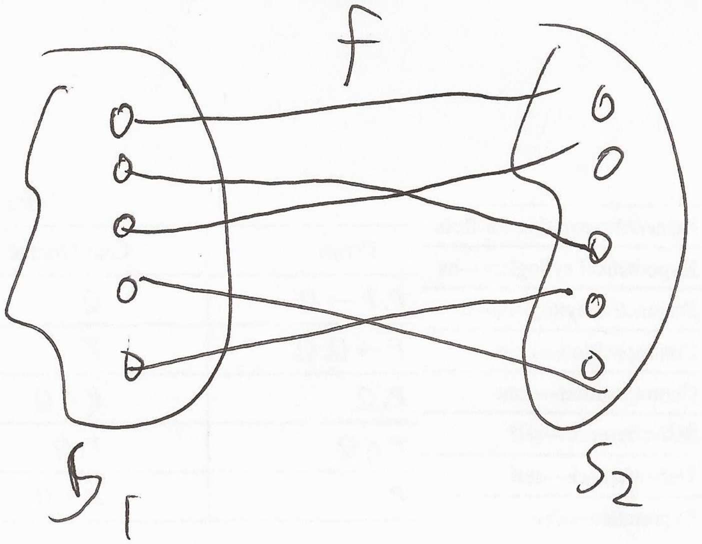
$z^{-1} \circ (z \circ x) = z^{-1} \circ (z \circ y)$ using inverse

$(z^{-1} \circ z) \circ x = (z^{-1} \circ z) \circ y$ Using associativity

$i \circ x = i \circ y$ Using definition of inverse

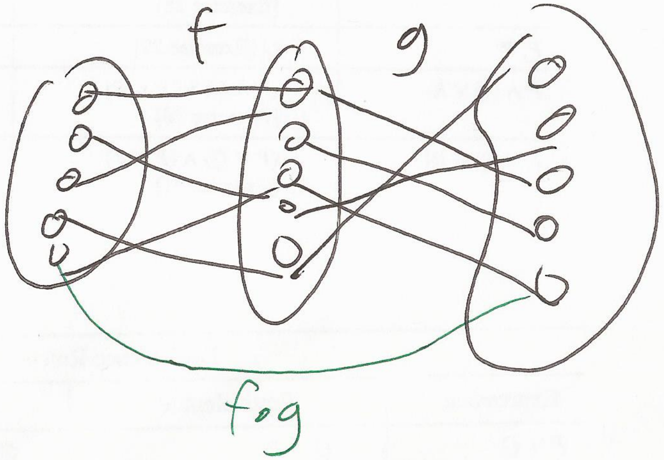
$x = y$ Using definition of identity

A bijection



Composition

$f \circ g \qquad f(g(x))$



We try to show that the set of function composition on ~~b~~ bijections is a group

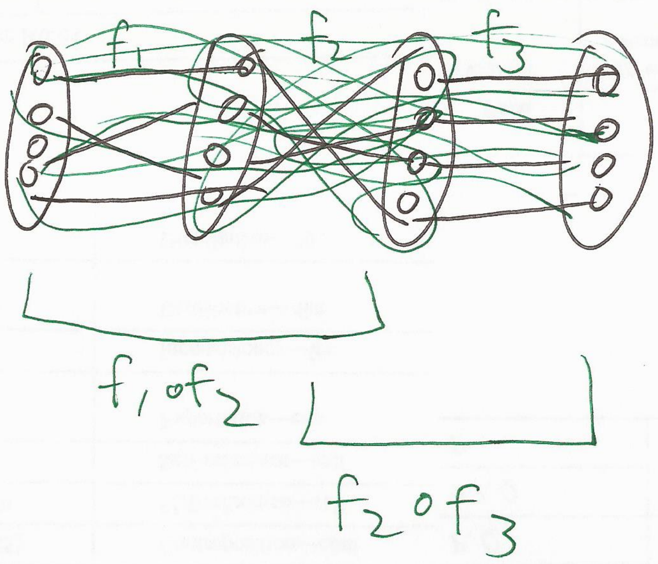
$\cancel{(\circ, B)}$ $\circ$ — composition

$B \rightarrow$ set of all bijections

$(\circ, B)$ is a structure.

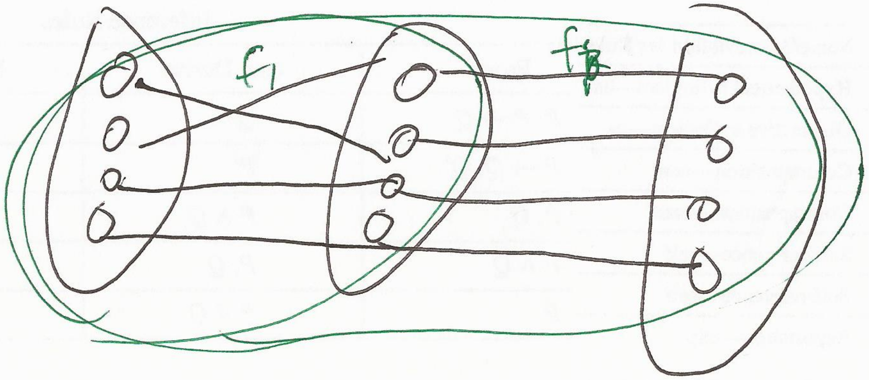
- $(\circ, B)$ is associative

$$(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$$



so $(\circ, B)$ is a semigroup

• (O,B) has an identity

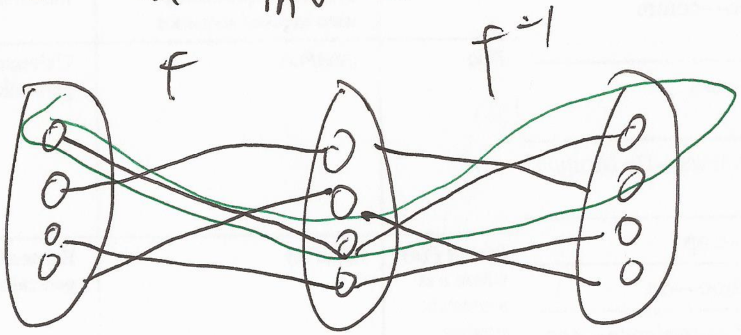


$f_1 \circ f_i = f_1$

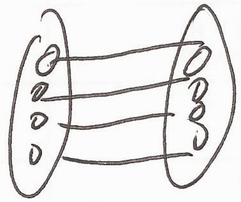
$f_i \circ f_1 = f_1$

(O,B) is a monoid

• (O,B) has an inverse.



→



f_i

$f \circ f^{-1} = f_i$

(O,B) is a group