M403 - Fall 2013 - Enrique Areyan - HW1 (1)

60/60

1. Let S be a set and let $f: S \to S$ be a function.

(a) ($\Rightarrow$) Suppose f is one-to-one.
Define a function $g: S \to S$ such that for $x \in S$:

$$g(x) = \begin{cases} f^{-1}(x) & \text{if } x \in Img(f); \quad Img(f) = \{y \in S \mid f(x) = y, \text{ for some } x \in S\} \\ a & \text{if } x \notin Img(f); \quad a \text{ is any fixed element of } S \end{cases}$$

Claim: $g(x)$ is a well-defined function. Pf: Let $x \in S$.
Clearly, if $x \notin Img(f)$, then $f(x) = a$, where a is a fixed element of S and thus g in this case is well-defined.
Otherwise, if $x \in Img(f)$ then $f(x)$ is a unique element since f is one-to-one, i.e. $\forall x, y \in S: f(x) = f(y) \Rightarrow x = y$. therefore, it makes sense to use the inverse of f only when $x \in Img(f)$, so that $f(f^{-1}(x)) =$
this shows that g is well defined over S. End of claim.

To show that g is the function we want (left inverse of f),
let $x \in S$. then:

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \\ &= f^{-1}(f(x)) \quad \text{since } f(x) \in Img(f) \text{ and definition of } g. \\ &= x \end{aligned}$$

Hence, $g \circ f = id$.

($\Leftarrow$) Suppose that there exists a function $g: S \to S$ such that $g \circ f = id$
Let $x, y \in S$. be such that $f(x) = f(y)$. then.

$$\begin{aligned} f(x) &= f(y) && \text{apply } g \text{ to both sides} \\ g(f(x)) &= g(f(y)) \\ (g \circ f)(x) &= (g \circ f)(y) && \text{By definition of function composit} \\ x &= y && \text{Since } g \circ f = id. \end{aligned}$$

Hence, f is one-to-one.

(b) ($\Rightarrow$) Suppose f is onto, i.e., $\forall y \in S : \exists x \in S$ s.t. $f(x) = y$
Define the function $g: S \to S$ such that for an arbitrary element $y \in S$
$g(y) = x$ if and only if $f(x) = y$. Since f is onto we know that such an element $f(x) = y$ exist $\forall y \in S$. If there are more than one (as we are not assuming f to be one-to-one) then pick one (any).

Then, for any $y \in S$: $(f \circ g)(y) = f(g(y))$ By composition of func
$= f(x)$ By construction of g.
$= y$

Hence, $f \circ g = id$. Good

($\Leftarrow$) Suppose that there exists a function $g: S \to S$ such that $f \circ g = id$
Let $x \in S$. then $(f \circ g)(x) = f(g(x))$
$= x$

So that $\forall x \in S : \exists y \in S$, in particular $y = g(x)$, s.t. $f(y) = x$.

Hence, f is onto. Good

Part c is done easily by using the result of a and

(c) ($\Leftarrow$) Suppose that there exists a function $g: S \to S$ such that $f \circ g = g \circ f = id$. We want to prove: i) f is one-to-one and ii) f is onto.

i) Let $x, y \in S$ be such that $f(x) = f(y)$. Apply g to both sides:
$g(f(x)) = g(f(y)) \Leftrightarrow (g \circ f)(x) = (g \circ f)(y) \Leftrightarrow x = y$. Hence, f is 1-

ii) Let $x \in S$. then $(f \circ g)(x) = f(g(x)) = x$. So that there exists $y = g(x) \in S$ s.t. $f(y) = x$. Hence, f is onto.

($\Rightarrow$) Suppose that f is one-to-one and onto. Define $g: S \to S$ for an arbitrary element $x \in S$ to be: $g(x) = y \Leftrightarrow x = f(y)$

<u>claim</u>: g is a well-defined function. Using ideas developed before:

<u>Pf</u>: Since f is onto: given $y \in S$ we can always find $x \in S$ s.t. $f(x) = y$. Moreover, since f is one-to-one, such x is uniquely determin

<u>End of claim</u>

Finally, show that g is both left and right inverse.

Given $x \in X$: $g(x) = y$ By def of g.

$f(g(x)) = f(y)$ Apply f to both sides

$(f \circ g)(x) = x$ Hence, $f \circ g = id$.

+10

Likewise, $y \in X$: $f(y) = x$ By def

$g(f(y)) = g(x)$ Apply g to both sides

$(g \circ f)(y) = y$ Hence, $g \circ f = id$

therefore, $f \circ g = g \circ f = id$. (g is the inverse of f).

(d) Let $T = \{f : \mathbb{N} \to \mathbb{N}\}$ (set of functions from $\mathbb{N}$ to $\mathbb{N}$).
with usual function composition as the associative operation.
As we know, there is an identity for this set: $id : \mathbb{N} \to \mathbb{N}$; $id(n) = n$
since, for any $f \in T$: $(f \circ id)(n) = f(id(n)) = f(n) = id(f(n)) = (id \circ f)(n)$.

the following element is left invertible:

$f : \mathbb{N} \to \mathbb{N}$ where $f(n) = n+1$.

its left inverse is:

$g : \mathbb{N} \to \mathbb{N}$ where $g(n) = 0$ if $n = 0$; otherwise $g(n) = n-1$ if $n > 0$

Note that g is a member of T since $g(0) = 0 = g(1) \in \mathbb{N}$, so g takes values in the proper codomain.

Moreover, g is a left inverse of f since:
For any $n \in \mathbb{N}$: $(g \circ f)(n) = g(f(n)) = g(n+1) = (n+1)-1 = n$, since $n+1 > 0$

But f does not have a right inverse, since f is not onto (part (b) of this exercise). To show that f is not onto:

Let $n = 0$. Find n' s.t $f(n') = 0$. But $f(n') = n'+1 = 0$
$\Rightarrow n' = -1 \notin \mathbb{N}$. $\not\text{I}$

M403 - Fall 2013 - Enrique Areyan - HW1

2. Let S be a finite set and let $f: S \to S$ be a function.

Note that it suffices to show that $(a) \Rightarrow (b)$ and $(b) \Rightarrow (a)$, and all other implications will follow. this is because.

Suppose $(a) \Leftrightarrow (b)$ (which will be proved next).

then: $(a) \Rightarrow (c)$ since $(a) \Rightarrow (b)$ and $(a) \wedge (b) \Rightarrow (c)$. Likewise
$(b) \Rightarrow (c)$ since $(b) \Rightarrow (a)$ and $(a) \wedge (b) \Rightarrow (c)$.

Other implications are trivial (e.g. $(c) \Rightarrow (a) \wedge (b)$).

Now let us prove $(a) \Leftrightarrow (b)$.

$(a) \Rightarrow (b)$. Suppose f is one-to-one. For a contradiction, suppose that f is not onto. then $|Im(f)| < |S|$ ... By definition: $Im(f) = \{y \in S : f(x) = y$ for some $x \in S\}$. Since S is a finite set, we can label all its elements as follow: $s_1, s_2, \ldots, s_n$ where $n = |S|$. Now, look at $|Img(f)|$. Since f is one-to-one and all of $s_1, s_2, \ldots, s_n$ are distinct elements. then $f(s_1), f(s_2), \ldots, f(s_n)$ must be distinct elements. But then

We can then form the set $Im(f) = \{f(s_1), f(s_2), \ldots f(s_n)\}$.

$$|Img(f)| = |\{f(s_1), f(s_2), \ldots, f(s_n)\}| = n = |S| < |S|$$, by previous assumption

this is a clear contradiction and thus, f is onto.

$(b) \Rightarrow (a)$. Suppose f is onto. For a contradiction, suppose that f is not one-to-one. In a similar argument as before, first note that $|Img(f)| = |S|$, since f is onto. Look at the set:

$Img(f) = \{f(s_1), f(s_2), \ldots, f(s_n)\}$. Since f is not one-to-one there exists distinct elements s_i, s_j with $i \neq j$, $1 \leq i, j \leq n$. such that $f(s_i) = f(s_j)$. In particular, this means that there are at least two elements in $Img(f)$ that are really the same. Hence

$|Img(f)| = |S| \leq |S| - 1$; a contradiction. thus, f is one-to-one.

M403 - Fall 2013 - Enrique Areyan - HW1

3. Let $(G, \#)$ be a group and let H be a nonempty finite subset of G. Prove that H is a subgroup of G if and only if H is closed under $\#$.

Pf: $(\Rightarrow)$ Suppose that H is a subgroup of G. then by definition of subgroup H is closed under $\#$.

$(\Leftarrow)$ Suppose that H is closed under $\#$.

Here we will adopt the usual notation for powers of an element in a group, i.e., $\underbrace{h\#h\#\cdots\#h}_{k \text{ times}} = h^k$, for $k \in \mathbb{N}$ and $k \geq 1$.

$h^0 = e$ identity of G.

$\underbrace{h^{-1}\#h^{-1}\#\cdots\#h^{-1}}_{\ell \text{ times}} = h^{-\ell}$ (with usual power laws)

Claim: $e \in H$.

(we can pick an $h \in H$ because H is nonempty)

Pf: Consider the sequence: $h, h^2, h^3, \ldots, h^n, \ldots$. Since H is closed under $\#$ and it is finite, we know there must be at least one repetition in this sequence. Let $m > n$ be positive integers such that $h^m = h^n$ the element h^n has an inverse in G because $h^n \in G$ and G is a group. Apply h^{-n} to both sides of $h^m = h^n$:

$$h^m = h^n \Rightarrow h^m \# h^{-n} = h^n \# h^{-n} = e, \text{ by properties of } G.$$
$$\Rightarrow h^{m-n} = e.$$

Since $m > n$ is true that $m - n > 0$. So let $t = m - n$ a positive integer. We have found a positive power of h to be the identity $h^t = h^{m-n} = e \in H$, since all positive powers of h are in H. End of claim

claim: for any $h \in H \Rightarrow h^{-1} = h^{m-n} \# h^{-1} = h^{m-n-1}$, with m, n picked as before.

Pf: $h \# h^{m-n-1} = h^{1+m-n-1} = h^{m-n} = e = h^{m-n-1+1} = h^{m-n-1} \# h$

Note that by our choice of m, n, $m > n \Rightarrow m - n > 0 \Rightarrow m - n \geq 1$ $\Rightarrow m - n - 1 \geq 0$. So that $h^{m-n-1} = h^{-1} \in H$, since h^{m-n-1} is a positive power of h. therefore, all element $h \in H$ have an inverse $h^{-1} = h^{m-n-1}$, where m, n depend on the choice of h. this proves that H is a subgroup of $(G, \#)$ (Note that e is its own inverse $e = h^{m-n}$, so $e \in H \Rightarrow e^{-1} \in H$).

4. Let G be a set with an associative operation that satisfies th
two properties:

(a) $\exists e \in G : ge = g \ \forall g \in G$.

(b) $\forall g \in G : \exists h \in G : gh = e$.

Prove that G is a group under this operation.

Pf: Need to prove the following three properties:

(1) the operation is associative

(2) $\exists t \in G : \forall g \in G : tg = gt = g$

(3) $\forall g \in G : \exists g^{-1} \in G : gg^{-1} = g^{-1}g = g$

(1) is given to us as a hypothesis.

(3) Two cases:

(i) e is the only element in G. then e is its own inverse : $ee = e$

(ii) there exists some other element in G distinct from e.

~~there exists some other element in G distinct from e~~

Let $g \in G$. by (b) there exists $h \in G$ s.t $gh = e$. But, since $h \in G$, by (b) there exists $s \in G$ s.t: $hs = e$. therefore:

$$\underset{\text{by (a)}}{hg = (hg)e} \underset{hs=e}{=} (hg)(hs) \underset{\text{associativity}}{=} h((gh)s) \underset{gh=e}{=} h(es) \underset{\text{associativity}}{=} (he)s = hs = e$$

therefore; Given $g \in G$, the element h provided in (b) is its inverse since

$$gh = hg = e$$

(2) Like before, two cases:

(i) e is the only element in G then e is the identity $ee = e$

(ii) Let $g \in G$. by (b) there exists $h \in G$ s.t $gh = e$. Moreover, there exists $s \in G$ s.t. $hs = e$ (by (b)). Hence:

$$eg = (gh)g = g(h(ge)) = g(h(g(hs))) = g(h((gh)s)) = g(h(es)) = g(hs) = ge = g$$

So the element e provided in (a) is the identity since $eg = ge = g$.

therefore, G is a group under this operation.

5. Write down the group table for D_4.

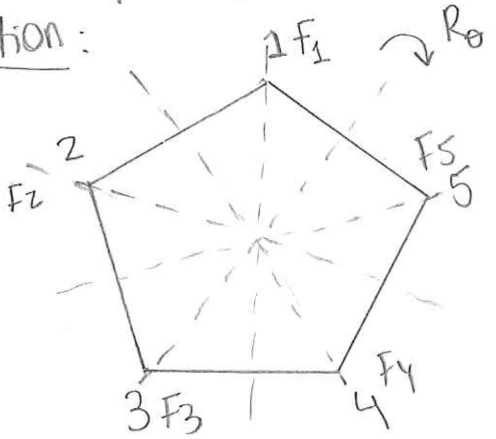
Solution: Let $D_4 = \{I, R_1, R_2, R_3, D_1, D_2, H, V\}$

	I	R_1	R_2	R_3	D_1	D_2	H	V
I	I	R_1	R_2	R_3	D_1	D_2	H	V
R_1	R_1	R_2	R_3	I	V	H	D_1	D_2
R_2	R_2	R_3	I	R_1	D_2	D_1	V	H
R_3	R_3	I	R_1	R_2	H	V	D_2	D_1
D_1	D_1	H	D_2	V	I	R_2	R_1	R_3
D_2	D_2	V	D_1	H	R_2	I	R_3	R_1
H	H	D_2	V	D_1	R_3	R_1	I	R_2
V	V	D_1	H	D_2	R_1	R_3	R_2	I

---

6. Determine the elements of D_5, the group of symmetries of the regular pentagon.

Solution:



F_i = reflection through corner i

R_θ = rotation of angle θ

From the picture we can conclude that there are 10 elements in D_5, including the identity: $I = \begin{pmatrix} 1&2&3&4&5 \\ 1&2&3&4&5 \end{pmatrix}$.

Hence: $D_5 = \{I, R_{72^\circ}, R_{144^\circ}, R_{216^\circ}, R_{288^\circ}, F_1, F_2, F_3, F_4, F_5\}$

these elements act on the corner of the pentagon as follow:

$F_1 = \begin{pmatrix} 1&2&3&4&5 \\ 1&5&4&3&2 \end{pmatrix}$; $F_2 = \begin{pmatrix} 1&2&3&4&5 \\ 3&2&1&5&4 \end{pmatrix}$; $F_3 = \begin{pmatrix} 1&2&3&4&5 \\ 5&4&3&2&1 \end{pmatrix}$; $F_4 = \begin{pmatrix} 1&2&3&4&5 \\ 2&1&5&4&3 \end{pmatrix}$

$F_5 = \begin{pmatrix} 1&2&3&4&5 \\ 4&3&2&1&5 \end{pmatrix}$; $R_{72^\circ} = \begin{pmatrix} 1&2&3&4&5 \\ 5&1&2&3&4 \end{pmatrix}$; $R_{144^\circ} = \begin{pmatrix} 1&2&3&4&5 \\ 4&5&1&2&3 \end{pmatrix}$; $R_{216^\circ} = \begin{pmatrix} 1&2&3&4&5 \\ 3&4&5&1&2 \end{pmatrix}$; $R_{288^\circ} = \begin{pmatrix} 1&2&3&4 \\ 2&3&4&5 \end{pmatrix}$