MIDTERM III – SOLUTIONS

Q1]... [25 points] How would you start to write down a proof that some set X is a subset of some other set Y? In other words, what is the key fact that you have to prove?

We must show $\forall x \, (x \in X \longrightarrow x \in Y)$

So start with any $x \in X$, and prove $x \in Y$.

Suppose that A, B, C are sets. Write down a proof that if $A \subset B$, then $C - B \subset C - A$. Be sure to justify each step of your proof.

We are given (hypotheses) $A \subset B$

This means: $x \in A \Rightarrow x \in B$ --- def of "$\subset$"

Equivalently $x \notin B \Rightarrow x \notin A$ --- contrapositive.

Now given $x \in C - B$

This means "$x \in C$ and $x \notin B$" --- defn of "set difference".

But $x \notin B \Rightarrow x \notin A$ --- established above.

Thus "$x \in C$ and $x \notin A$"

i.e. $x \in C - A$ --- defn of "set difference"

We've shown $x \in C - B \Longrightarrow x \in C - A$

Thus $(C - B) \subset (C - A)$

∎

Q2]... [25 points] Say whether the following functions are *only injective*, *only surjective*, *bijective*, or *neither injective nor surjective*. It is important for you to give reasons for your answers.

1. $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (m, n) \mapsto 5^m 7^n$.

injective?

$f(m,n) = f(a,b)$

$\Rightarrow 5^m 7^n = 5^a 7^b$

Fundamental Th^{m} of Arithmetic (uniqueness)

$\Rightarrow m = a$ & $n = b$

$\Rightarrow (m,n) = (a,b)$

Thus f is injective

surjective? Given $2 \in \mathbb{N}$.

is $2 = f(m,n)$ for some (m,n)?

ie. is $2^1 = 5^m 7^n$

Again Fund. Th^{m} says No!
(otherwise we contradict prime decomp of 2)

$\Rightarrow$ f is NOT surjective

$\boxed{f \text{ is only injective}}$

2. $g : \mathbb{Z} \to \mathbb{Z} : x \mapsto 3x - 4$.

injective?

$g(x) = g(y)$

$\Rightarrow 3x - 4 = 3y - 4$

$\Rightarrow 3x = 3y$ ... (adding 4)

$\Rightarrow x = y$ ... (dividing by 3)

$\Rightarrow$ g is injective

surjective?

Given z

$g(x) = z$ means $3x - 4 = z$

$\Rightarrow 3x = z + 4$

$x = \frac{z+4}{3}$

But this is not always in $\mathbb{Z}$

eg. $z = 0 \Rightarrow x = \frac{4}{3} \notin \mathbb{Z}$

So g is NOT surjective.

$\boxed{g \text{ only injective}}$

3. $h : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto 3x + 4y$.

injective?

No! eg $h(4,0) = 12$

$h(0,3) = 12$

yet $(4,0) \neq (0,3)$

surjective?

Given $z \in \mathbb{R}$

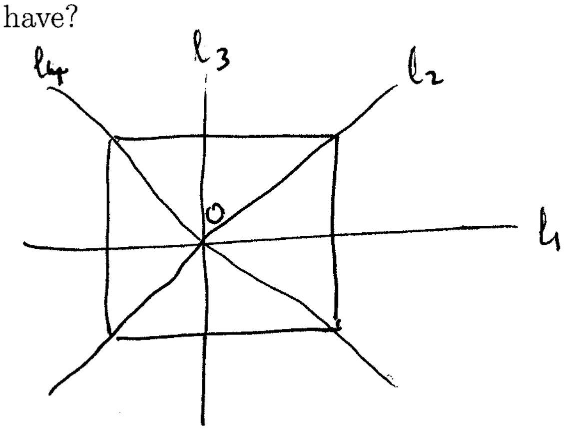
$\frac{z}{4} \in \mathbb{R}$ too.

& $h(0, \frac{z}{4}) = z$

$\Rightarrow$ h is surjective

$\boxed{h \text{ is only surjective}}$

Q3]... **[25 points]** List the elements of the group G of symmetries of a square. How many elements does G have?



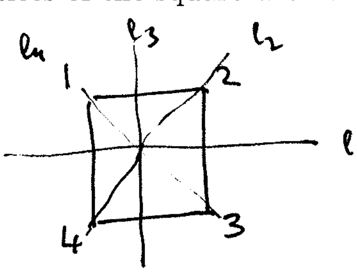
Let R = rotation about O, counterclockwise through $\pi/2$ radians.

$G = \mathrm{Symm}(\square)$ has 8 elements:

$$\mathbb{1},\ R,\ R^2,\ R^3,\ l_1,\ l_2,\ l_3,\ l_4$$

here l_i denotes "reflection in the line l_i".

Find *two distinct subgroups* of Perm($\{1,2,3,4\}$) which are isomorphic to the group G above. Write down explicit bijections between G and these subgroups of Perm($\{1,2,3,4\}$). [Hint: Think about ways of labeling the vertices of the square with the numbers 1, 2, 3, 4.]

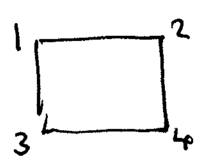


$\mathbb{1} \leftrightarrow \mathbb{1}$
$R \leftrightarrow (14\,32)$
$R^2 \leftrightarrow (13)(42)$
$R^3 \leftrightarrow (12\,34)$
$l_1 \leftrightarrow (14)(23)$
$l_2 \leftrightarrow (13)$
$l_3 \leftrightarrow (12)(34)$
$l_4 \leftrightarrow (24)$

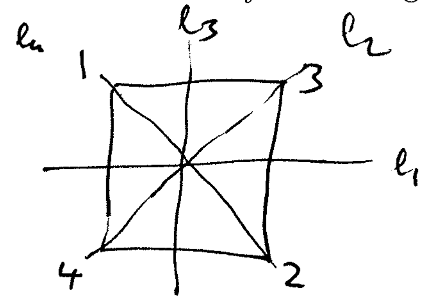
one subgroup $H_1 < \mathrm{Perm}(\{1,2,3,4\})$.

Note:

There is a 3rd subgroup! corresponding to the ordering



of vertices



$\mathbb{1} \leftrightarrow \mathbb{1}$
$R \leftrightarrow (14\,23)$
$R^2 \leftrightarrow (12)(34)$
$R^3 \leftrightarrow (1324)$
$l_1 \leftrightarrow (14)(23)$
$l_2 \leftrightarrow (12)$
$l_3 \leftrightarrow (13)(24)$
$l_4 \leftrightarrow (34)$

2nd subgroup $H_2 < \mathrm{Perm}(\{1,2,3,4\})$

Q4]... [**25 points**] Say whether the following are True or False. Give a short reason (phrase, name of a theorem, example) for your answers.

1. Order((12345)) = 5.

$\boxed{T}$

$(12345)^2 = (1\,3\,5\,2\,4) \neq 1$

$(12345)^3 = (12345)(13524) = (14253) \neq \mathbb{1}$

$(12345)^4 = (12345)(14253) = (15432) \neq \mathbb{1}$

$(12345)^5 = (12345)(15432) = \mathbb{1}$.

Order $\stackrel{\text{def.}}{\equiv}$ smallest ⊕ power giving $\mathbb{1}$.

2. $\mathbb{Z}_{10} - \{0\}$ is a group under multiplication.

$\boxed{F}$

$2, 5 \in \mathbb{Z}_{10} - \{0\}$ but $2.5 = 10 \equiv 0 \pmod{10}$

"Not closed under ×". $\notin \mathbb{Z}_{10} - \{0\}$

3. The set of all subsets of a finite set A has $2^{|A|}$ elements.

$\boxed{T}$

This property of $P(A)$ was proven in class (by induction on $n = |A|$)

4. If A has n elements, then the set of all *injective functions* from A to A has $n!$ elements.

$\boxed{T}$

There is n choices for $f(1)$

There is $(n-1)$ ------ $f(2)$ --- given a choice for $f(1)$

There is $(n-2)$ ---- $f(3)$ -- given choices for $f(1), f(2)$

---.etc---

$\Rightarrow$ $n!$ possible injective functions!

5. $|A \cup B| = |A| + |B|$.

$\boxed{F}$

eg $A = \{1,2\}$ $B = \{2\}$ $|A \cup B| = |\{1,2\}| = 2$

$\neq 2 + 1$

6. $\{\emptyset\} - \emptyset = \{\}$.

$\boxed{F}$

$\emptyset$ and $\{\}$ are both the <u>empty set</u>.

But $\{\emptyset\}$ is not the empty set (it has one element, namely $\emptyset$)

$\{\emptyset\} - \emptyset = \{\emptyset\} \neq \{\}$.