Q1]... **[20 points]** Solve the following system of congruences. Show the details of your work.

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 2 \mod 9 \\ x &\equiv 3 \mod 5 \end{aligned}$$

Use the Chinese Remainder Theorem (given to us on the sheet!)...

$z_1 = (9)(5) = 45$

$z_2 = (4)(5) = 20$

$z_3 = (4)(9) = 36$

$z_1 \equiv 1 \mod 4 \Rightarrow y_1 = z_1^{-1} \equiv 1 \mod 4$

$z_2 \equiv 2 \mod 9 \Rightarrow y_2 = z_2^{-1} \equiv 5 \mod 9$

$z_3 \equiv 1 \mod 5 \Rightarrow y_3 = z_3^{-1} \equiv 1 \mod 5$

$(2)(5) \equiv 1 \mod 9$

Finally

$X = y_1 z_1 a_1 + y_2 z_2 a_2 + y_3 z_3 a_3$

$= (1)(45)(1) + (5)(20)(2) + (1)(36)(3)$

$= 45 + 200 + 108$

$= 353$

$\equiv 173 \mod 180$

$(4)(9)(5) = 180$

$$\begin{array}{r} 353 \\ -180 \\ \hline 173 \end{array}$$

Answer $\boxed{x = 173 \mod 180}$

Mid III SOLUTIONS

Q2]... **[20 points]** Let $f : X \to Y$ be a function, and suppose that $A \subseteq X$.

1. Prove that $A \subseteq f^{-1}(f(A))$.

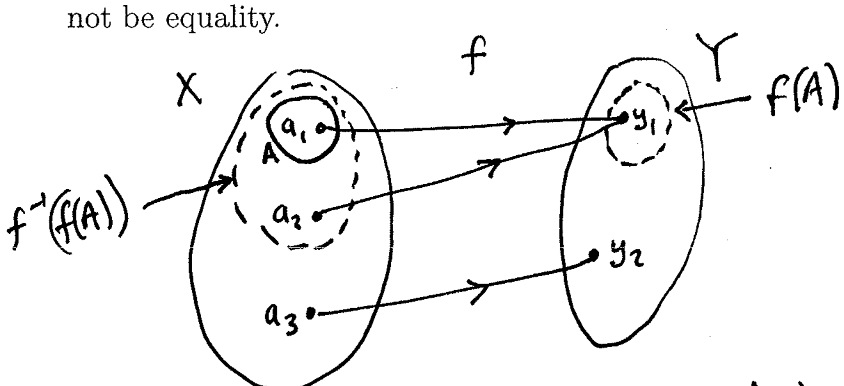
Let $a \in A$. Then $f(a) \in f(A)$ ... by def$^{\underline{n}}$ of image of a subset of X.

But $a \in A$ & $f(a) \in f(A) \implies a \in f^{-1}(f(A))$ ... by def$^{\underline{n}}$ of the premage of a subset of Y.

We've shown $a \in A \implies a \in f^{-1}(f(A))$

& so $A \subseteq f^{-1}(f(A))$ -- by def$^{\underline{n}}$ of subset inclusion. $\boxtimes$

2. Give an explicit example of f, X, Y and $A \subseteq X$ which demonstrates that the inclusion above need not be equality.



$X = \{a_1, a_2, a_3\}$ $Y = \{y_1, y_2\}$

$f : a_1 \mapsto y_1 ; a_2 \mapsto y_1 ; a_3 \mapsto y_2$

$A = \{a_1\}$

$f(A) = \{f(a_1)\} = \{y_1\}$

$f^{-1}(f(A)) = f^{-1}(\{y_1\}) = \{a_1, a_2\}$

Note $\{a_1\} \subsetneqq \{a_1, a_2\}$

3. One of the extra hypotheses f *is injective* or f *is surjective* will guarantee that the inclusion above is actually an equality of sets. Which one? Give a short proof that equality holds under your additional hypothesis.

<u>f is injective</u>.

We've proven $A \subseteq f^{-1}(f(A))$ in item 1 above.

In order to establish equality, we must prove $f^{-1}(f(A)) \subseteq A$.

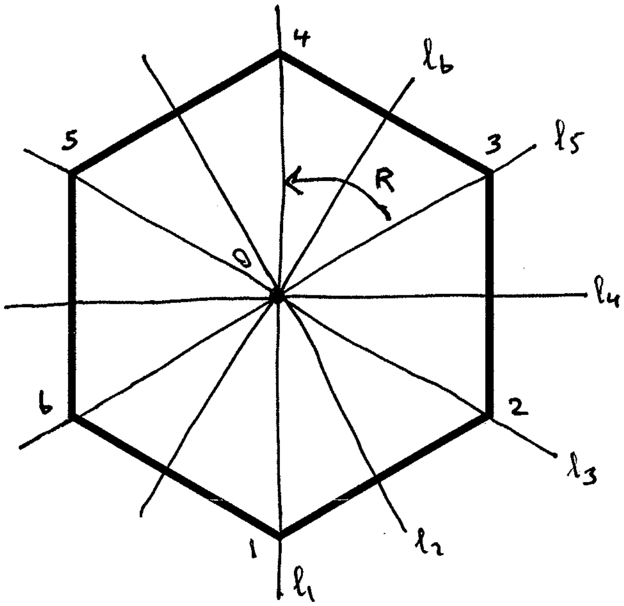
Let $x \in f^{-1}(f(A))$. By def$^{\underline{n}}$ of premage, this means $f(x) \in f(A)$.

By def$^{\underline{n}}$ of image, this means $f(x) = f(a)$ for some $a \in A$.

Now we have elements $x, a \in A$ such that $f(x) = f(a)$. The hypothesis that f is <u>injective</u> implies that $x = a$ & so $x \in A$.

$\Rightarrow f^{-1}(f(A)) \subseteq A$. $\boxtimes$

Q3]... [20 points] Describe and list the elements of the group, D_6, of symmetries of the regular hexagon below. Use the space to the right of the image for your answer. You can draw on the diagram too.



l_i = reflection in the line l_i (drawn).

R = rotation counterclockwise about O through $\frac{2\pi}{6} = \frac{\pi}{3}$ radians.

$$D_6 = \{\mathbb{I}, R, R^2, R^3, R^4, R^5, l_1, l_2, l_3, l_4, l_5, l_6\}$$

Find an isomorphism between D_6 and a subgroup of the symmetric group S_6. Say why your correspondence preserves multiplication.

Step ① Label the vertices of the hexagon (for example, as shown).

Step ② If $f \in D_6$, f is a bijective map of $\mathbb{R}^2$ which sends the set of 6 vertices $\{1, \dots, 6\}$ into itself. $\Rightarrow$ get element of S_6.

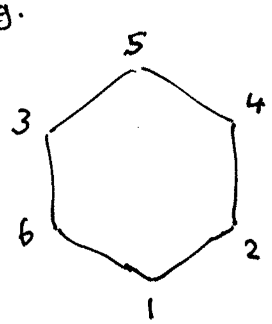
Since the perm corresponding to f is just equal to f with its domain + codomain restricted, then composition of rigid motions will correspond to composition of permutations. Here is the explicit correspondence.

$\mathbb{I} \leftrightarrow \mathbb{I}$; $R \leftrightarrow (123456)$; $R^2 \leftrightarrow (135)(246)$; $R^3 = (14)(25)(36)$; $R^4 \leftrightarrow (153)(264)$; $R^5 \leftrightarrow (654321)$; $l_1 \leftrightarrow (26)(35)$; $l_2 \leftrightarrow (12)(36)(45)$; $l_3 \leftrightarrow (13)(46)$; $l_4 \leftrightarrow (14)(23)(56)$; $l_5 \leftrightarrow (15)(24)$; $l_6 \leftrightarrow (16)(25)(34)$.

Find an isomorphism between D_6 and a different subgroup of S_6.

Choose a different labeling of vertices of hexagon:

eg.



$\mathbb{I} \leftrightarrow \mathbb{I}$

$R \leftrightarrow (124536)$

$R^2 \leftrightarrow (143)(256)$

$R^3 \leftrightarrow (15)(23)(46)$

$R^4 \leftrightarrow (134)(265)$

$R^5 \leftrightarrow (635421)$

$l_1 \leftrightarrow (26)(34)$

$l_2 \leftrightarrow (12)(46)(35)$

$l_3 \leftrightarrow (14)(56)$

$l_4 \leftrightarrow (15)(24)(36)$

$l_5 \leftrightarrow (13)(25)$

$l_6 \leftrightarrow (16)(23)(45)$

Q4]... [40 points] For each of the following statements, say whether it is true (T) or false (F). Make sure that you give short arguments to support your choice in each case (either providing a counterexample, or a short proof or computation or a connection to a result from the course).

1. $\{\emptyset\} = \emptyset$ $\boxed{F}$ the set on the left $\{\emptyset\}$ is not empty; it contains one element, $\emptyset$.

2. If $A = \{1, 2, 3\}$, then $\emptyset \in A$. $\boxed{F}$ there are only 3 elements in A; 1, 2, 3.

3. $12345^{67894} \equiv 4 \mod 11$. $\boxed{T}$

$12345 \equiv 5-4+3-2+1 \equiv 3 \mod 11$

$67894 \equiv 4 \mod 10$

$10 = 11-1$
11 is prime

Fermat Little Th^m

Fermat $\Rightarrow$ $12345^{67894} \equiv 3^4 \mod 11$

$\equiv 9^2 \mod 11 \equiv 81 \equiv 4 \mod 11$

4. The following product of permutations is correct.

$$(12345)(2531) = (45)(123)$$

$\boxed{F}$

$1 \mapsto 2 \mapsto 3 \Rightarrow$ $1 \to 3$ does not agree with RHS

5. The following product of permutations is correct. $\boxed{T}$

$$(123456)(135)(24)(654321) = (246)(35)$$

$(654321) = (123456)^{-1}$ $\Rightarrow$ LEFT SIDE IS CONJUGATION by (123456)

Call it f.

Answer is $(f(1)\ f(3)\ f(5))\ (f(2)\ f(4))$

$\|$

$(2\ 4\ 6)(3\ 5)$ ✓

6. If $f : X \to Y$ is a function and $A \subseteq X$, $B \subseteq X$, then

$$f(A \cap B) = f(A) \cap f(B)$$

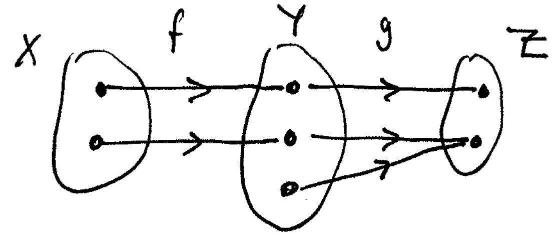
$\boxed{F}$ see below for diagram

$X = \{1,2,3\}$ $\quad Y = \{y, z\}$ $\quad A = \{1,2\}$ $\quad B = \{2,3\}$

$f : 1 \mapsto y \quad 2 \mapsto z \quad 3 \mapsto y$ $\qquad A \cap B = \{2\}$

7. Suppose $f : X \to Y$ and $g : Y \to Z$ are functions. If $g \circ f$ is bijective, then f and g are both bijective.

$\boxed{F}$



$g \circ f$ is bijective

f not surjective

g not injective

8. If $A \neq \emptyset$ and $A \times B = A \times C$, then $B = C$.

$A \neq \emptyset \Rightarrow \exists\, a \in A.$ (You need an element $a \in A$ to make this work!)

If $b \in B$, then $(a,b) \in A \times B = A \times C$

$\Rightarrow (a,b) \in A \times C$

$\Rightarrow b \in C$ $\qquad \Rightarrow \boxed{B \subseteq C}$

If $c \in C$, then $(a,c) \in A \times C = A \times B$

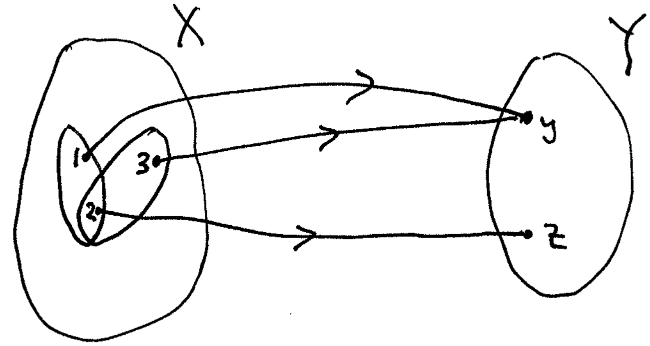
$\Rightarrow (a,c) \in A \times B$

$\Rightarrow c \in B$

$\Rightarrow \boxed{C \subseteq B}$

$\Rightarrow B = C$

Picture for Example 6 ...



$f(A \cap B) = f(\{2\})$
$= \{z\}$

$f(A) \cap f(B) = \{y,z\} \cap \{y,z\}$
$= \{y,z\}$

NOT EQUAL!