8/23

$\mathbb{Z}$, $a \sim b$ if $3 \mid (a-b)$

$\sim$ an equivalence relation on $\mathbb{Z}$

$\mathbb{Z} = [0] \cup [1] \cup [2]$ (disjoint union)

$m \in \mathbb{Z}_{>1}$

For $a, b \in \mathbb{Z}$, define

$a \sim b$ if $m \mid (a-b)$

Then $\sim$ is an equivalence relation.

$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$

$a \sim b$, $m \mid (a-b) \Rightarrow a - b = mk$

$\Rightarrow a = mk + b$

We say $a \equiv b \bmod m \Leftrightarrow a = mk + b$.

"congruent to" same as $\sim$

Since $\sim$ is an equivalence relation, we have

(1) $a \equiv a \bmod(m)$

(2) $a \equiv b \bmod(m) \Rightarrow b \equiv a \bmod(m)$

(3) $a \equiv b \bmod(m)$, $b \equiv c \bmod(m)$

$\Rightarrow a \equiv c \bmod(m)$

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

$$\mathbb{Z}/_{\sim} = \{[0], [1], \cdots, [m-1]\}$$

$$= \{\underline{0}, \underline{1}, \cdots, \underline{m-1}\}$$

$\{0, 1, 2, \cdots, m-1\}$ = set of integers modulo m.

$= \mathbb{Z}_m$

Ex (1) $\mathbb{Z}_3 = \{0, 1, 2\}$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Lattin square

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Not Lattin square.

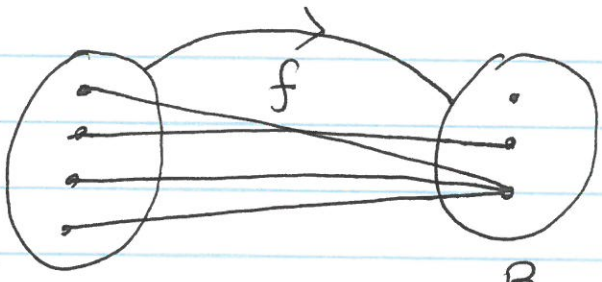
Ex (2) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Lattin square

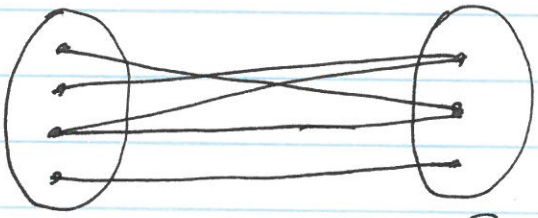
$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Not a Lattin square

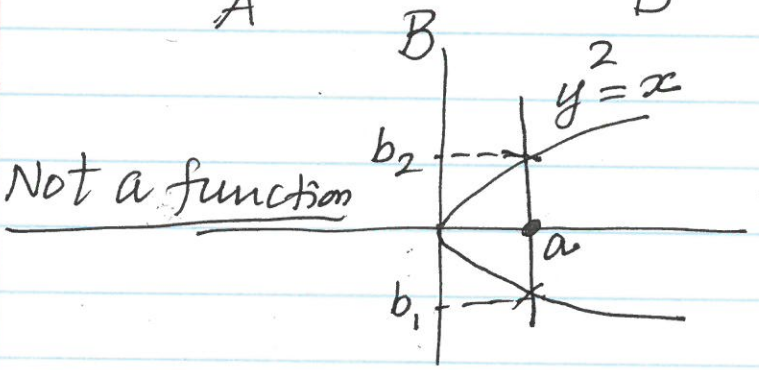


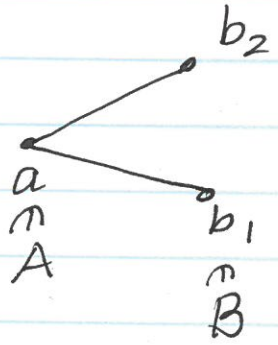
function

domain codomain



Not function





A, B nonempty sets and $f: A \to B$ a function.

(1) One-to-one: $f: A \to B$ is 1-1 if $f(a) = f(b) \Longrightarrow a = b$.

(2) Onto: $f: A \to B$ is <u>onto</u> if for each $b \in B$, there is $a \in A$ such that $f(a) = b$.

(3) A function $f: A \to B$ is a bijection if f is 1-1 and onto.

Ex(1) $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$

One to One? $f(n) = f(m)$
yes. $\quad 2n = 2m \Rightarrow n = m$

Onto? $\quad 3 \in \mathbb{Z}$
no. $\quad f(n) = 3 \Rightarrow 2n = 3$ which is impossible for any $n \in \mathbb{Z}$.

Ex(2) $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = |n|$

One-to-one? $\quad f(2) = |2| = 2 = |-2| = f(-2)$
No. $\quad 2 \neq -2$

Onto? $\quad -2 \in \mathbb{Z}$
No. $\quad f(n) = |n| \geq 0$, $f(n) \neq -2$ for any $n \in \mathbb{Z}$

HW: P23 #1, 2, 3, 4, 6, 8, 9, 11, 12, 15, 18, 19, 20, 21, 27, 28, 34, 35, 58, 59, 60.

P24 #9

$a' = a \bmod(n) \Rightarrow a = mn + a'$

$b' = b \bmod(n) \Rightarrow b = \kappa n + b'$

$(a+b) = (m+\kappa)n + (a'+b')$

$\Rightarrow (a+b) \bmod(n) = (a'+b') \bmod(n)$

$ab = (mn+a')(\kappa n + b')$

$= \underbrace{mn\kappa n + a'\kappa n + b'mn}_{''} + a'b'$

$= (m\kappa n + a'\kappa + b'm)n + a'b'$

$\Rightarrow ab \bmod(n) = a'b' \bmod(n)$

#8. $d = \gcd(a,b)$, $a = da'$, $b = db'$

$\Rightarrow d = sa + tb$, $s, t \in \mathbb{Z}$.

$= sda' + tdb'$

$= d(sa' + tb')$

$\Rightarrow 1 = sa' + tb' \Rightarrow \gcd(a', b') = 1$.

#20. $P_1, P_2, \cdots, P_n$ prime

$P_i \nmid (P_1 P_2 \cdots P_n) + 1$ for $1 \le i \le n$

Suppose $P_i \mid (P_1 P_2 \cdots P_n) + 1$ for some i.

$$(P_1 P_2 \cdots P_n) + 1 = d P_i$$

$$\Rightarrow \quad 1 = d P_i - P_1 P_2 \cdots P_n$$

$$= P_i \left(d - P_1 \cdots P_{i-1} P_{i+1} \cdots P_n \right)$$

$\Rightarrow \quad P_i \mid 1$ contradiction since $P_i \geq 2$.

#21. Suppose we have finitely many primes: $P_1 < P_2 < \cdots < P_n$

$\Rightarrow \quad P_i \nmid (P_1 P_2 \cdots P_n) + 1$ for any $1 \leq i \leq n$

$\Rightarrow$ either $(P_1 P_2 \cdots P_n) + 1 \; (> P_i)$ is a prime or it has a prime factor $P > P_i$, $1 \leq i \leq n$

which is a contradiction.

Composition of functions:

$f : A \longrightarrow B$, $g : B \longrightarrow C$ functions

Then $(g \circ f) : A \longrightarrow C$

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

Note $g \circ f \neq f \circ g$.

Prop: $f: A \to B$, $g: B \to C$, $h: C \to D$

Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Prop: $f: A \to B$, $g: B \to C$

1) f & g are one-to-one then $g \circ f: A \longrightarrow C$ is one-to-one.

2) f & g are onto then $g \circ f$ is also onto.

Suppose $f: A \longrightarrow B$ one-to-one and onto

Then define $f^{-1}: B \to A$ by

$$f^{-1}(b) = a \iff f(a) = b.$$

called the inverse of f.

Clearly, $(f^{-1} \circ f): A \longrightarrow A$ and

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

$\Rightarrow f^{-1} \circ f = id_A$, similarly, $f \circ f^{-1} = id_B$

S be any nonempty set.

$P(S)$ = set of all 1-1 and onto maps from S to S.

Then we have:

(1) For all $f, g \in P(S)$, $g \circ f \in P(S)$

(2) For all $f, g, h \in P(S)$,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(3) $1 = id_S \in P(S)$ and

$1 \circ f = f$, $f \circ 1 = f$ for $f \in P(S)$

(4) For each $f \in P(S)$, there is $f^{-1} \in P(S)$ such that

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

$(P(S), \circ)$ is a group.

Group: A group is a nonempty set with an operation $*$ (called "multiplication") satisfying:

(1) $\forall\ a, b \in G$, $a * b \in G$ (closure)

(2) $\forall\ a, b, c \in G$, $(a * b) * c = a * (b * c)$ (associativity)

(3) $\exists$ unique $e \in G$ such that (identity element)

$$a * e = a = e * a \quad \forall a \in G.$$

(identity)

(4) For each $a \in G$ there exists unique $a^{-1} \in G$ such that

$$a * a^{-1} = e = a^{-1} * a$$ (inverse)

Example: (1) $(P(S), \circ)$ group

(2) $(\mathbb{Z}, +)$ group.

P24 #18

$$8^{402} \bmod 5 = (8^2)^{201} \bmod 5$$

$$= 64^{201} \bmod 5 = 4^{201} \bmod 5$$

$$= (-1)^{201} \bmod 5 = -1 \bmod 5 = 4 \bmod 5 = 4$$

$(G, *)$ group

- $\forall a, b \in G \Rightarrow a * b \in G$ (closure)
- $\forall a, b, c \in G \Rightarrow a*(b*c) = (a*b)*c$ (associativity)
- $\exists!\ e \in G$ such that $a * e = a = e * a$ $\forall a \in G$ (identity)
- For each $a \in G$, $\exists!\ a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$ (inverse)

Ex:

(1) $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}, +)$ groups

(2) $(\mathbb{Z}_p, +_p)$ group.

(3) $(\mathbb{Z}, \cdot)$ not a group.

Defn: A group G is **abelian** if

$$\forall\ a, b \in G \Rightarrow a * b = b * a.$$

Ex (1) $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}, +), (\mathbb{Z}_p, +_p)$

abelian groups.

Ex (2) $S = \{1, 2, 3\}$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \alpha\circ\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\beta\circ\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha^2 = \alpha\circ\alpha = e, \quad \alpha\circ\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

$$\beta\circ\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \alpha\circ\beta$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$P(S) = \{e, \alpha, \beta, \alpha\circ\beta, \beta\circ\alpha, \beta^2\} := S_3$$

S_3 is not an abelian group.

Defn: The order of a group G is the number of elements in G, denoted by $|G|$.

Ex: (1) $|\mathbb{Z}_3| = 3$ $\quad (\mathbb{Z}_3 = \{0, 1, 2\})$

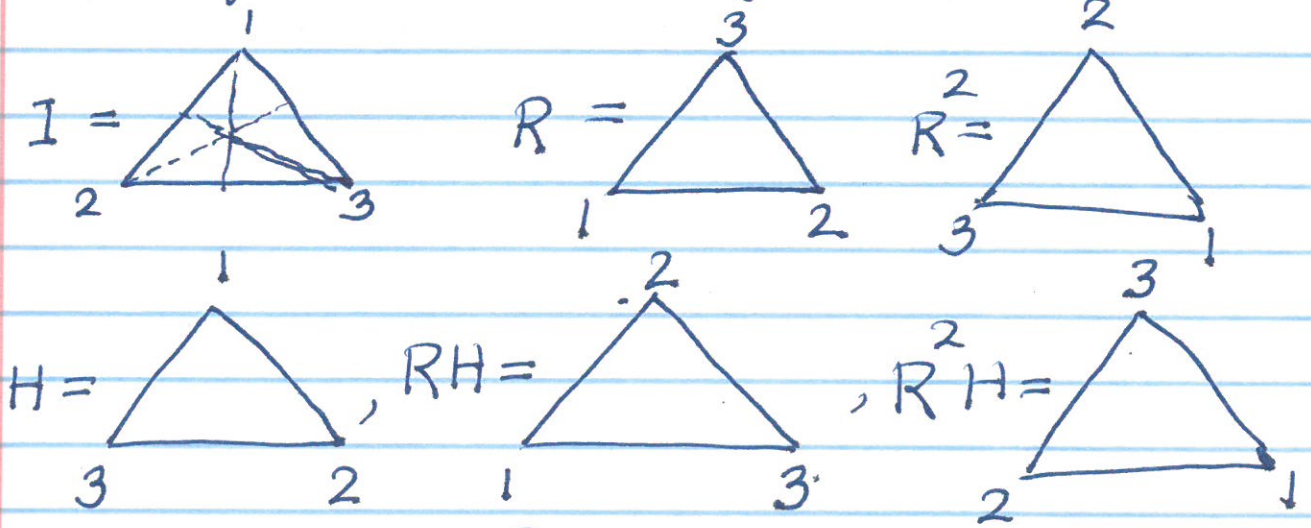
(2) $|S_3| = 6$ $\qquad$  $3 \times 2 \times 1 = 3!$

In general,

$$|S_n| = n!$$

Symmetries:

(1) Equilateral triangle:



$$D_3 = \{e = I, R, R^2, H, RH, R^2H\}$$

$$RH = HR^2 \qquad R^2H = HR$$

called the Dihedral group.

$|D_3| = 6$, D_3 is not abelian.

HW P37 # 2, 4, 11, 13, 14, 15