Week 2

§3 Modular arithmetic

Suppose S is a set.

In NSF, a relation R on S is defined to be a property that may, or may not, hold for each ordered pair of elements in S

(an element of $S \times S$)

Def A relation R on S

is **reflexive** if aRa holds for every element a of S

symmetric if aRb implies bRa for all elements a & b

in S

Transitive if aRb

and bRc

implies aRc

for all a, b, c

in S.

① $S = \mathbb{R}$

Define aRb if $a = b$

or $a = -b$

holds.

(2) $S = \mathbb{Z}$

$a R b$ if $ab = 0$

(3) $S = \mathbb{R}$

$a R b$ if $a^2 + a = b^2 + b$

(4) $S = \{\text{people in the world}\}$

aRb if a lives within

100km of b.

1 Is aRa? $\forall a \in S$

Yes. because $a = a$.

Does $aRb \Rightarrow bRa$

Yes. because

$aRb \Rightarrow$ $a = b$

or $a = -b$

$\Rightarrow \quad b = a$

or $\quad b = -a$

$\Rightarrow \quad b R a.$

Does aRb
bRc $\Rightarrow aRc$?

$aRb \Rightarrow a = b$ ①
or
$a = -b$ ②

$bRc \Rightarrow b = c$ ③ or $b = -c$ ④

If ① & ③ holds then $a=b=c$

① & ④ holds then $a=b=-c$

② & ③ holds then $a=-b=-c$

② & ④ holds then $a=-b=c$

In all cases, $a=c$

or $a=-c$.

So it is an equiv. relation

(2) It is NOT!

$a = 1$ then

aRa does NOT hold.

because $a \times a = 1 \times 1 = 1$

(3)

aRa holds because

- $a^2 + a = a^2 + a$

- Does $aRb \Rightarrow bRa$?

$a^2 + a = b^2 + b$

$\Rightarrow \; b^2+b = a^2+a.$

- Does aRb, bRc $\Rightarrow aRc$?

$a^2+a = b^2+b$
$b^2+b = c^2+c$ $\Rightarrow$ $a^2+a = c^2+c.$

Therefore this is an equiv relation.

④ This is <u>NOT</u> an equiv. relation.

Does $\begin{matrix} aRb \\ bRc \end{matrix} \Rightarrow aRc$?

For example $a \overset{80\,km}{\text{———}} b \overset{40\,km}{\text{———}} c$

this fails transitivity.

6 $S = \{\text{positive integers}\}$

aRb if ab is a square of a positive integer.

$a = 4 \quad b = 9$

$4 R 9$ because $4 \cdot 9 = 36 = 6^2$

$2^2 \cdot 5^2 \cdot 4^2$

$= 2 \cdot 5^2 \cdot 2 \cdot 4^2$

* $a = 2 \cdot 5^2 = 50$ $\quad$ $b = 2 \cdot 4^2 = 32$

$50 R 32$ because $50 \cdot 32 = 1600 = 40^2$

Is $a R a$?

Yes because $a \times a = a^2$.

Does $a R b \Rightarrow b R a$?

Yes because

$$aRb \Rightarrow ab \text{ is a square}$$

$$\Rightarrow ba \text{ is} \text{ —''—}$$

$$\Rightarrow bRa.$$

Does $\begin{matrix} aRb \\ bRc \end{matrix} \Rightarrow aRc$?

$aRb \Rightarrow ab = m^2$ ... (*)

for some positive integer m.

$bRc \Rightarrow bc = n^2$ ... (**)

for some positive integer n.

Multiplying ⊛ and ⊛⊛, we get

$$ab^2c = m^2n^2$$

Suffices to show that

b divides mn.

Indeed, if this holds,

$$ac = \frac{m^2n^2}{b^2} = \left(\frac{mn}{b}\right)^2$$

where mn/b is a positive integer.

How do we show b divides mn?

Suppose p is a prime number that divides b.

and let p^r be the highest power of p that divides b.

What we want follows if p^r divides mn.

as b is the product of these

prime factors.

Since p^r divides b,

p^{2r} divides b^2

(Since $b = p^r \cdot q$,

$b^2 = (p^r q)^2 = p^{2r} \cdot q^2$)

$\Rightarrow$ p^{2r} divides b^2

$\Rightarrow$ p^{2r} divides ab^2c

$\Rightarrow$ p^{2r} divides $m^2n^2 = (mn)^2$

$\Rightarrow$ p^r divides mn.

as desired.

More precisely, if

p^s is the highest power of

p dividing mn,

then p^{2s} is — " —

— " — $(mn)^2$

$$p^{2r} \mid (mn)^2 \Rightarrow p^{2r} \mid p^{2s}$$

$\Rightarrow \quad r \le s$

$\Rightarrow \quad p^r \mid mn$

If $\mathcal{R}$ is a relation on S,

and a is an element of S,

we write $[a]_{\mathcal{R}}$ or $[a]$

to mean the set

$$\{ b \in S \mid a \mathcal{R} b \} \subseteq S$$

a subset

In particular, if R is an equivalence relation on S,

We call $[a]$ the equivalence class represented by a.

Rk If R is an equivalence relation and aRb,

then $[a] = [b]$.

Any b in S s.t. aRb holds can represent the same equivalence class.

Why $[a] = [b]$?

To prove this, we need to show

(*) $[a] \subseteq [b]$

as well as

$[a] \supseteq [b]$.

We'll check (*).

To do this, we need to show

that any $c \in [a]$

also satisfies $c \in [b]$.

Since $c \in [a]$, it follows by def^n that aRc ... ♡

OTOH, we are given aRb

so bRa ... ♡♡

(since R is symmetric)

♡ & ♡♡ together with the transitivity of R

implies bRc, i.e. $c \in [b]$.

Exercise Check $[b] \leq [a]$

In preparation of a theorem to follow,
we need the following:

Def. Let S be a set.
A partion of S is a set $\mathcal{P}$
of subsets of S satisfying
the following properties:

* ϕ (the empty set) $\notin \mathcal{P}$

* If $A, B \in \mathcal{P}$

  (A and B are subsets of S)

  & if they are distinct,

  then $A \cap B = \phi$

* The union of all elements in $\mathcal{P}$ is S.

<u>Example</u> ◎ $S = \mathbb{Z}$

$$P = \{ \{\text{all even integers}\} \quad \{\text{all odd integers}\} \}$$

- $S = \{1, 2, 3, 4, 5\}$.

$$P = \{ \{1, 2, 3\}, \{4\}, \{5\} \}$$

$$P = \{ \{1, 2, 3\}, \{3, 4\}, \{5\} \}$$

is <u>NOT</u> a partition.

because $A = \{1, 2, 3\} \cap B = \{3, 4\} \neq \phi$.

Def Elements of a partion P are **parts** of P.

Theorem 9 (Equivalence relation theorem).

- Let R be an **equivalence** relation on S.

Then $\{[a]_R\}_{a \in S}$ defines a **partition** of S.

- Conversely, given any partition $\mathcal{P}$ of S,

there is a unique equivalence relation $\mathcal{R}$ on S

such that the parts of $\mathcal{P}$

are exactly $\{[a]_{\mathcal{R}}\}_{a \in S}$.

This $\mathcal{R}$ is defined as follows:

$a \mathcal{R} b$ if a and b lie

in the same part of $\mathcal{P}$.

Rk The theorem says

having an equivalence relation

is the same as having a partition.

Example $S = \{1, 2, 3\}$

Partitions	Equivalence relations	Equiv classes
$\{1, 2, 3\}$	$aRb \ \forall a, b \in \{1, 2, 3\}$	$[1] = [2]$

$\{\{1\},\{2,3\}\}$

$1R1$

$2R2$

$2R3$

$3R2$

$3R3$

$[3]$ $\parallel$ $[1]$

$[2]=[3]$

$\{\{2\},\{1,3\}\}$

$2R2$

$1R1$

$1R3$

$3R1$

$3R3$

$\{\{3\},\{1,2\}\}$

Exercise

$\{\{1\},\{2\},\{3\}\}$

$1R1$

$2R2$

$3R3$

$[1]$

$[2]$

$[3]$

$p \mid b$

does NOT

guarantee

$p \mid mn$

$p^r \mid b$

* GOAL

$$b = p^r q^s$$

WANT TO KNOW if $b \mid mn$

If $p^r \mid mn$

& $q^s \mid mn$

then $p^r q^s \mid mn$

b ="

If $p \mid mn$

$q \mid mn$

$pq \mid mn$