# *Ch 2. Basic Structures: Sets, Functions*
# *Ch 9. Relations*
## Equivalence Relations

**Sungwon Kang**

**Acknowledgement**
- [Rosen 19] Kenneth H. Rosen, for Discrete Mathematics & Its Applications (8th Edition), Lecture slides
- [Hunter 11] David J. Hunter, Essentials of Discrete Mathematics, 2nd Edition, Jones & Bartlett Publishers, 2011, Lecture Slides

# Ch 9. Relations

# Reflexivity, Symmetry and Transitivity of Relations

**Definition**

A relation R is called *reflexivity*, *symmetric* and *transitive* if it satisfies the following definitions, respectively.

*Reflexivity.* For any $a \in S$, $a\,R\,a$.

*Symmetry.* For any $a, b \in S$, $a\,R\,b \Leftrightarrow b\,R\,a$.

*Transitivity.* For any $a, b, c \in S$, if $a\,R\,b$ and $b\,R\,c$, then $a\,R\,c$.

Reflexive relations: $=$, $\leq$, $\subseteq$, “divides”, ...

Symmetric relations: $=$, ”is a sister of” but “divides”, $<$, $\leq$ are not.

Transitive relations: $=$, $\leq$, $<$, $\subseteq$, “is a sister of”, “divides” but “likes”, ... are not.

# Equivalence relations

## Definition

A relation $R$ on a set $S$ is an *equivalence relation* if it satisfies all three of the following properties.

1. *Reflexivity.*
2. *Symmetry.*
3. *Transitivity.*

In other words, an equivalence relation is a relation that is reflexive, symmetric, and transitive.

# Equivalence relations: examples

**Example 1.** The relation on $\mathbf{Z}$ defined by $=$ is an equivalence relation.

**Example 2.** Let $S$ be the set of all symbols of the form $\frac{x}{y}$, where $x$ and $y \neq 0$ are integers. In other words, $S = \left\{ \frac{x}{y} \mid x, y \in \mathbf{Z}, y \neq 0 \right\}$. Define a relation $R$ on $S$ as follows. For any elements $\frac{x}{y}$ and $\frac{z}{w}$ in $S$, $\frac{x}{y} \, R \, \frac{z}{w}$ if $xw = yz$. Then $R$ is an equivalence relation.

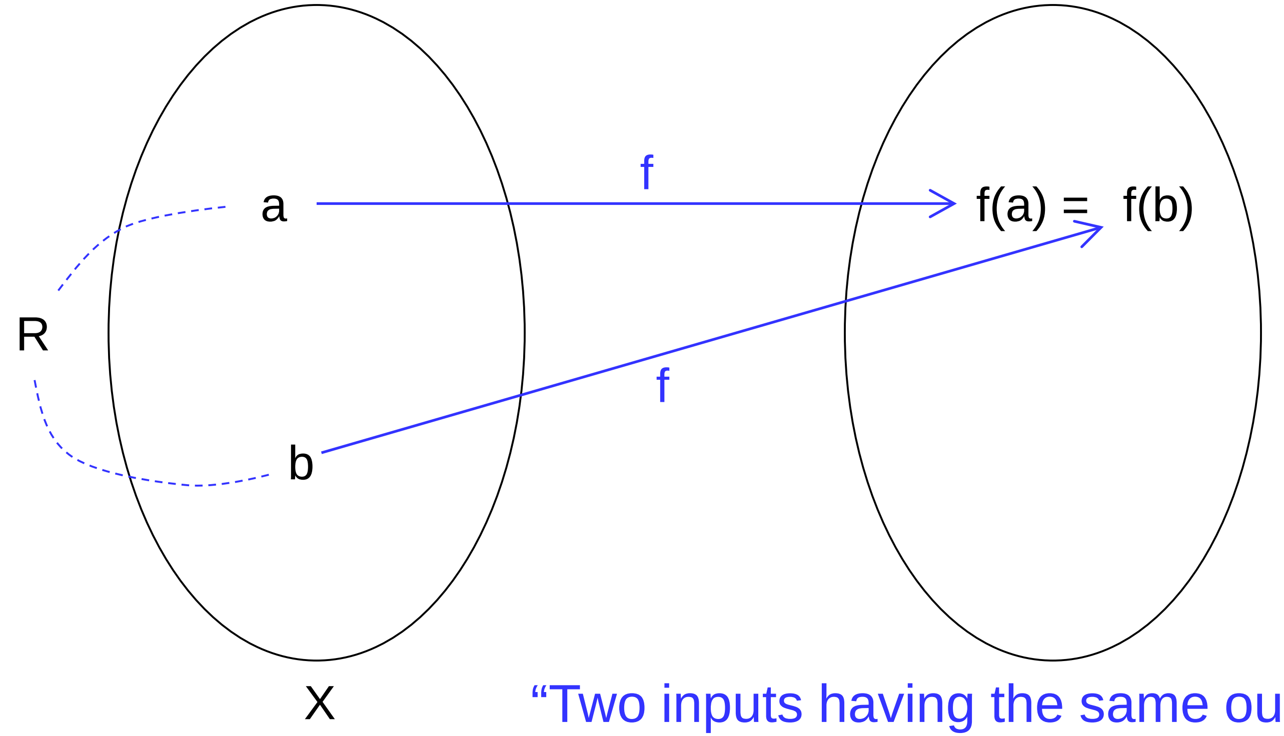
**Example 3.** Given any function $f : X \to Y$, define a relation on $X$ as follows. For any $a, b \in X$, $a \, R \, b$ if $f(a) = f(b)$. Then $R$ is an equivalence relation. (I.e. “Map to the same element” relation .)

How can we prove that a certain relation is an equivalence relation?

Given any function f: X→Y, define R as follows:

For any $a, b \in X$, define $a\,R\,b$ if $f(a) = f(b)$. The proof that $R$ is an equivalence relation has three parts:

**Proof.**




"Two inputs having the same output" relationship

## Given any function f: X →Y, define R as follows:

For any $a, b \in X$, define $a \, R \, b$ if $f(a) = f(b)$. The proof that $R$ is an equivalence relation has three parts:

**Proof.**

1. *Reflexivity.* Suppose that $a \in X$. Since $f$ is a well-defined function, $f(a) = f(a)$, so $a \, R \, a$.

## Given any function f: X →Y, define R as follows:

For any $a, b \in X$, define $a \, R \, b$ if $f(a) = f(b)$. The proof that $R$ is an equivalence relation has three parts:

**Proof.**

1. *Reflexivity.* Suppose that $a \in X$. Since $f$ is a well-defined function, $f(a) = f(a)$, so $a \, R \, a$.
2. *Symmetry.* Suppose that $a, b \in X$ and that $a \, R \, b$. By the definition of $R$, this means that $f(a) = f(b)$, which is the same thing as saying $f(b) = f(a)$. Thus $b \, R \, a$, as required.

## Given any function f: X →Y, define R as follows:

For any $a, b \in X$, define $a\,R\,b$ if $f(a) = f(b)$. The proof that $R$ is an equivalence relation has three parts:

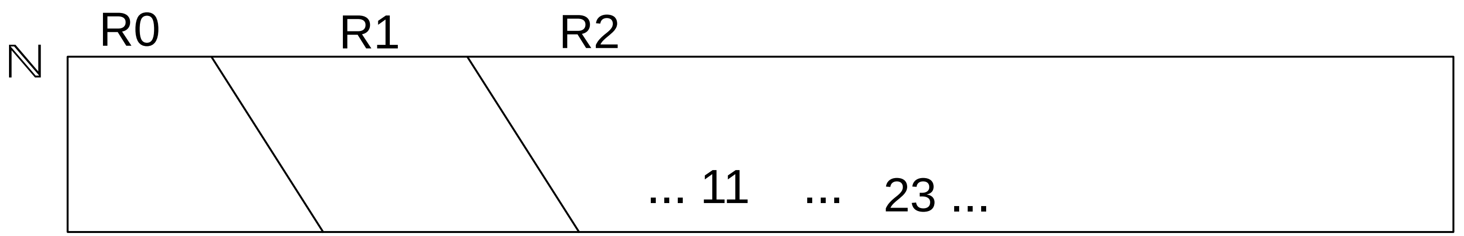
**Proof.**

1. *Reflexivity.* Suppose that $a \in X$. Since $f$ is a well-defined function, $f(a) = f(a)$, so $a\,R\,a$.
2. *Symmetry.* Suppose that $a, b \in X$ and that $a\,R\,b$. By the definition of $R$, this means that $f(a) = f(b)$, which is the same thing as saying $f(b) = f(a)$. Thus $b\,R\,a$, as required.
3. *Transitivity.* Let $a, b, c \in X$ with $a\,R\,b$ and $b\,R\,c$. Then $f(a) = f(b)$ and $f(b) = f(c)$, so by substitution, $f(a) = f(c)$. This shows that $a\,R\,c$.

□

**Exercise 1** We studied the "equivalence modulo n relation".

Is the "equivalence modulo 3 relation" an equivalence relation?




How can we prove it?

☛ 1) Directly proving the three properties of equivalence relation

2) The theorem we will study shortly can be used for this.

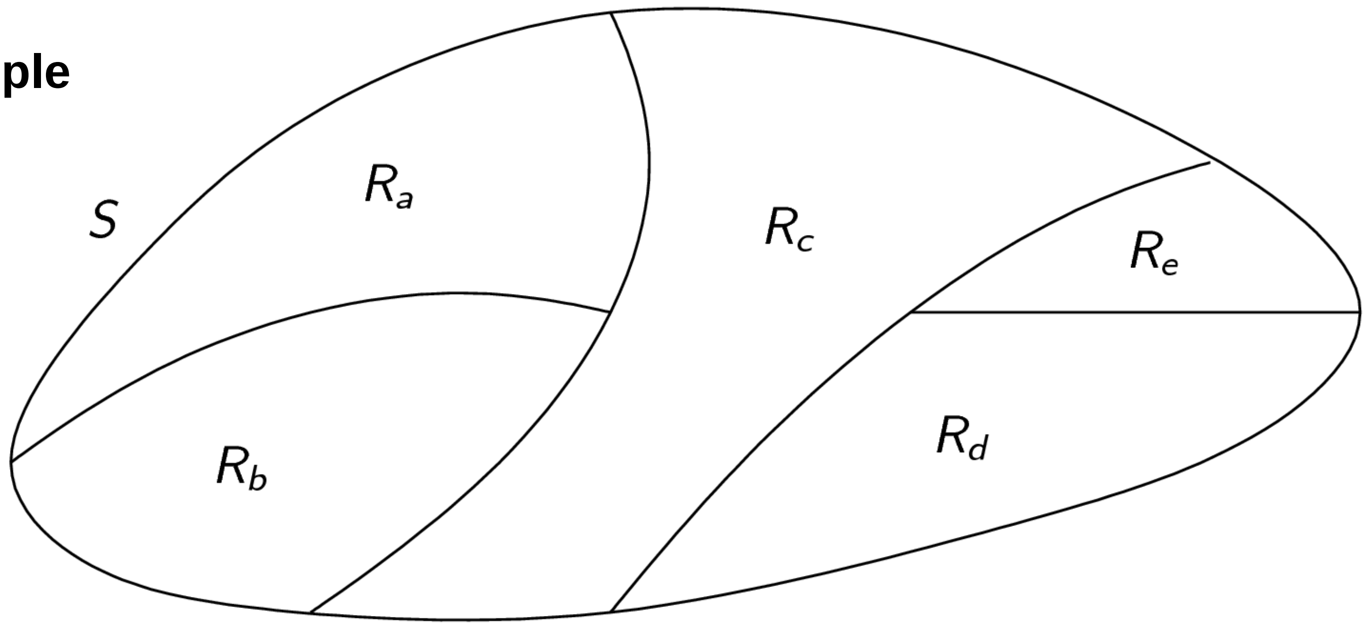
# Equivalence classes and partitions

**Definition** A *partition* of a set S is a set P of nonempty subsets of S with the following properties.

1. For any a ∈ S, there is some set X ∈ P such that a ∈ X. The elements of P are called the *blocks* of the partition. (P is exhaustive.)

2. If X, Y ∈ P are disjoint blocks, then X ∩ Y = ∅. (P has no overlapping blocks.)

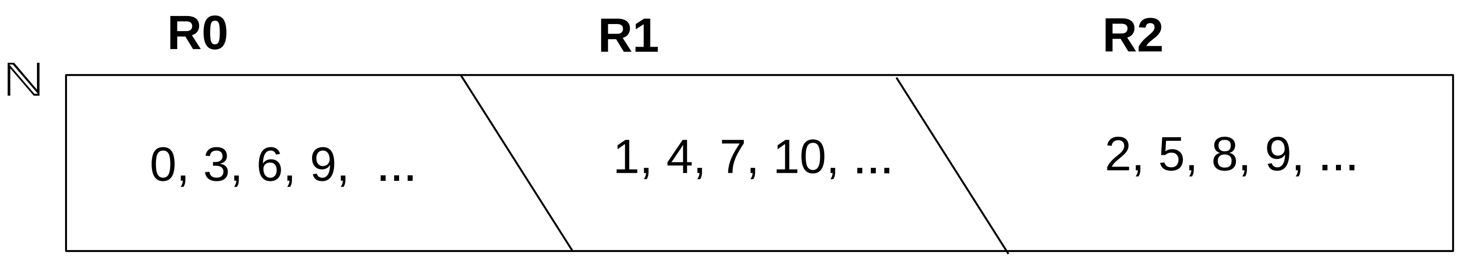
**Example**



0, 3, 6, 9, ... are all equivalent modulo 3
because if they are divided by 3 they all have the same remainder 0.
Call this set **R0**.

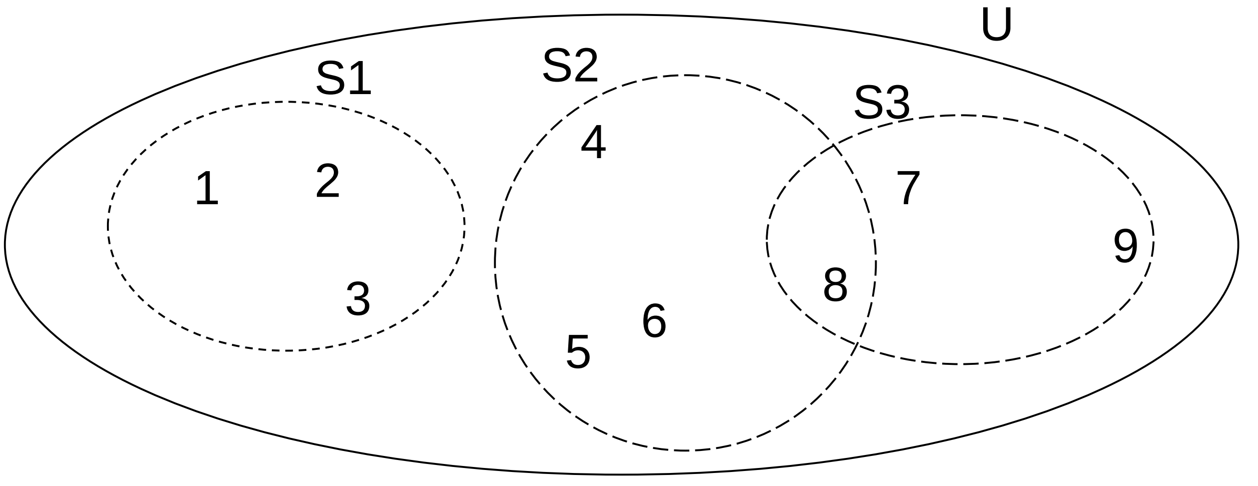
1, 4, 7, 10, ... are all equivalent modulo 3
because if they are divided by 3 they all have the same remainder 1.
Call this set **R1**.

2, 5, 8, 11, ... are all equivalent modulo 3
because if they are divided by 3 they all have the same remainder 2.
Call this set **R2**.



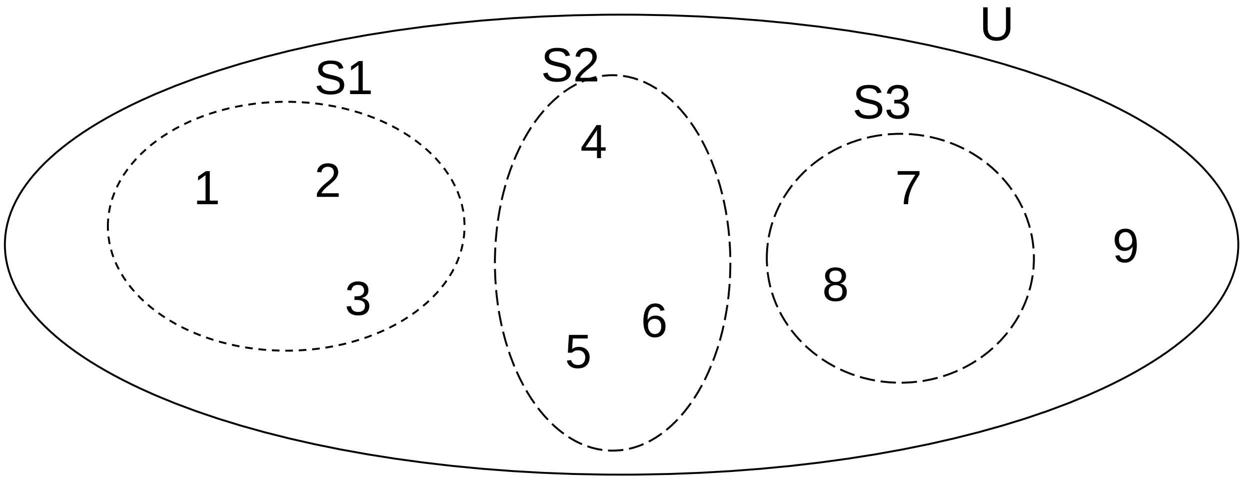

R0, R1 and R2 "partition" ℕ.

**Example 1** U = {1, 2, 3, 4, 5, 6, 7, 8, 9}



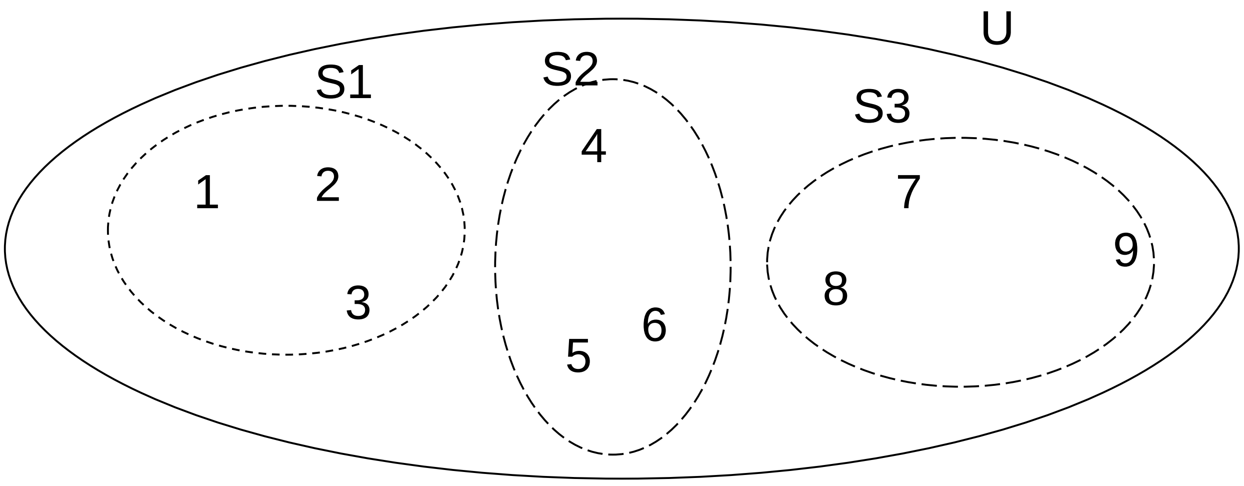

Is {S1, S2, S3} a partition of U?

**Example 2** U = {1, 2, 3, 4, 5, 6, 7, 8, 9}




Is {S1, S2, S3} a partition of U?

**Example 3** U = {1, 2, 3, 4, 5, 6, 7, 8, 9}




Is {S1, S2, S3} a partition of U?

# Equivalence classes and partitions

Called *the equivalence class of x with respect to R*.

**Theorem**

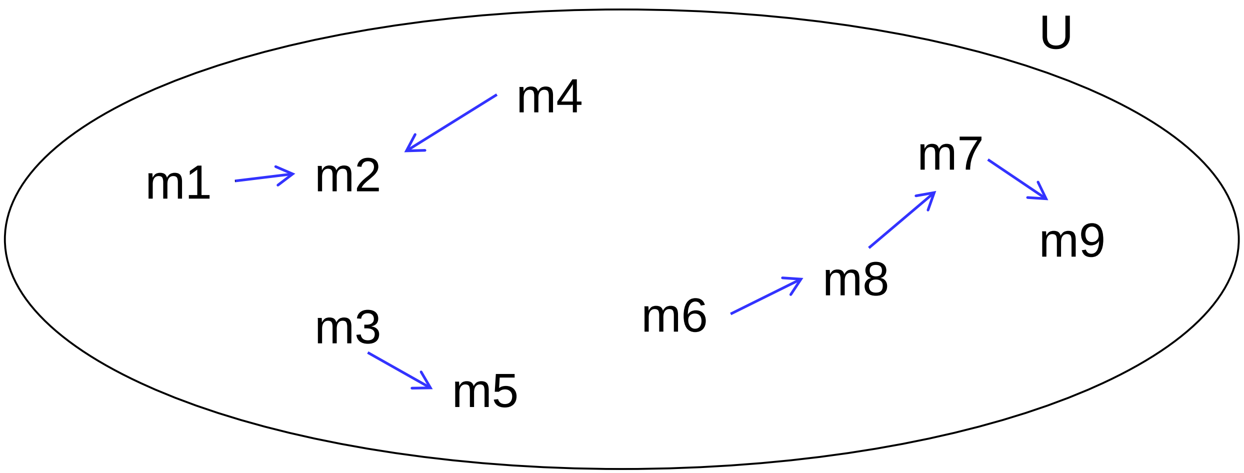
*Let $R$ be an equivalence relation on a set $S$. For any element $x \in S$, define $R_x = \{a \in S \mid x\,R\,a\}$, the set of all elements related to $x$. Let $P$ be the collection of distinct subsets of $S$ formed in this way, that is, $P = \{R_x \mid x \in S\}$. Then $P$ is a partition of $S$.*

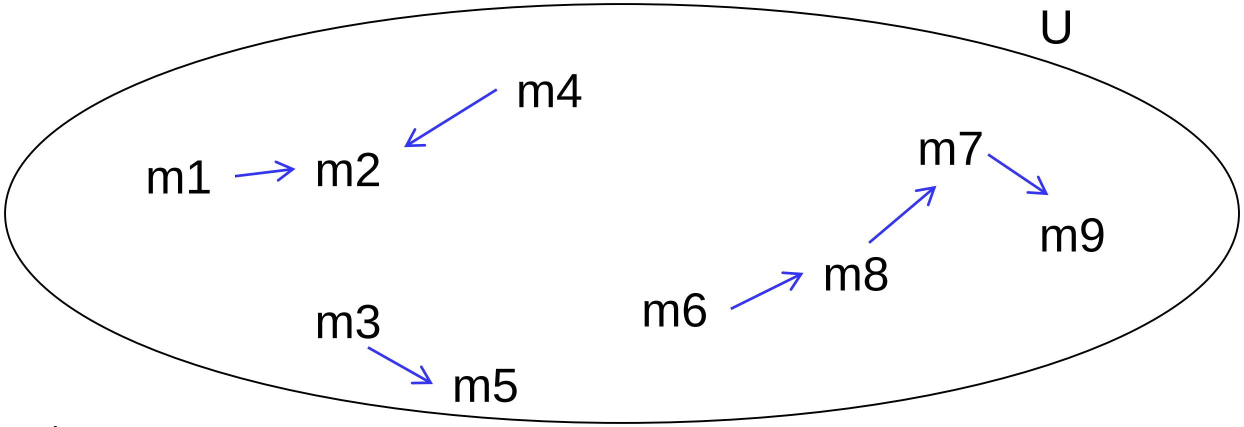
**Example 4** U = {m1, m2, m3, m4, m5, m6, m7, m8, m9}

It is the set of 9 weird monkeys.
A relation that makes them weird is the following:
1) Each monkey likes itself.
2) If monkey A likes another one B, then B likes A, too.
3) If A likes B and B likes C, then A likes C.

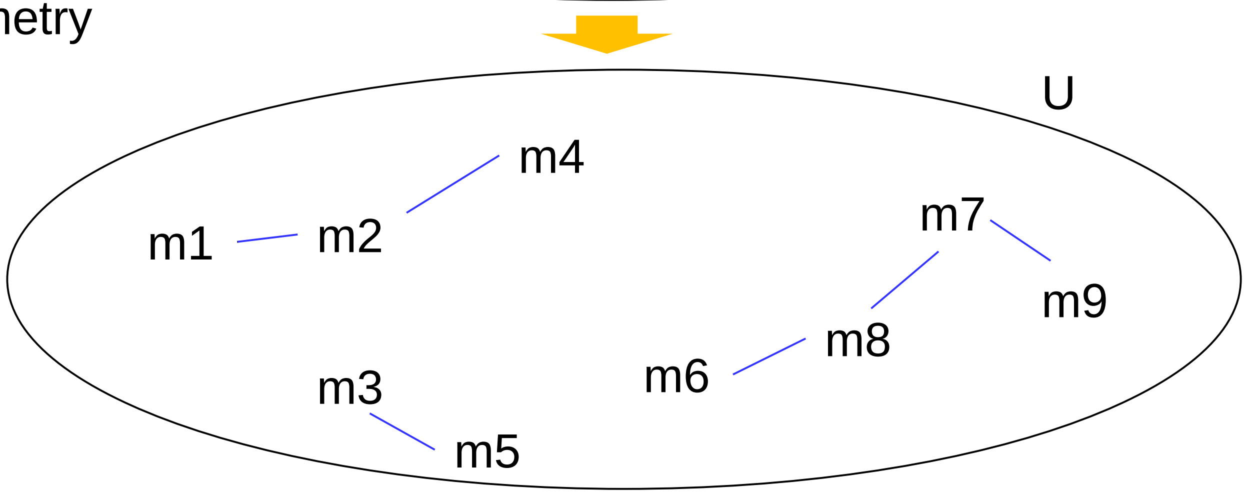
In this world, is the "likes" relation an equivalence relation?

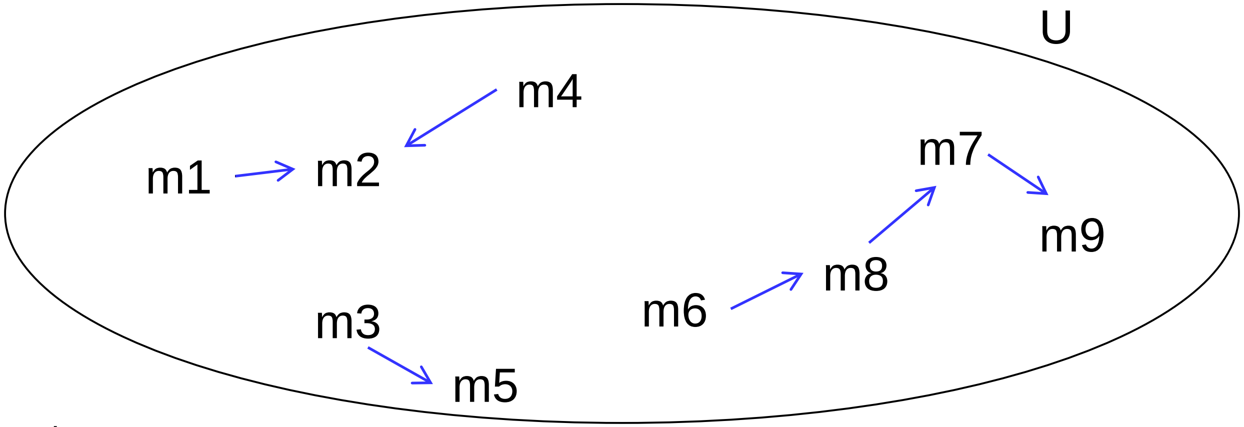
For example, we may know the following facts.



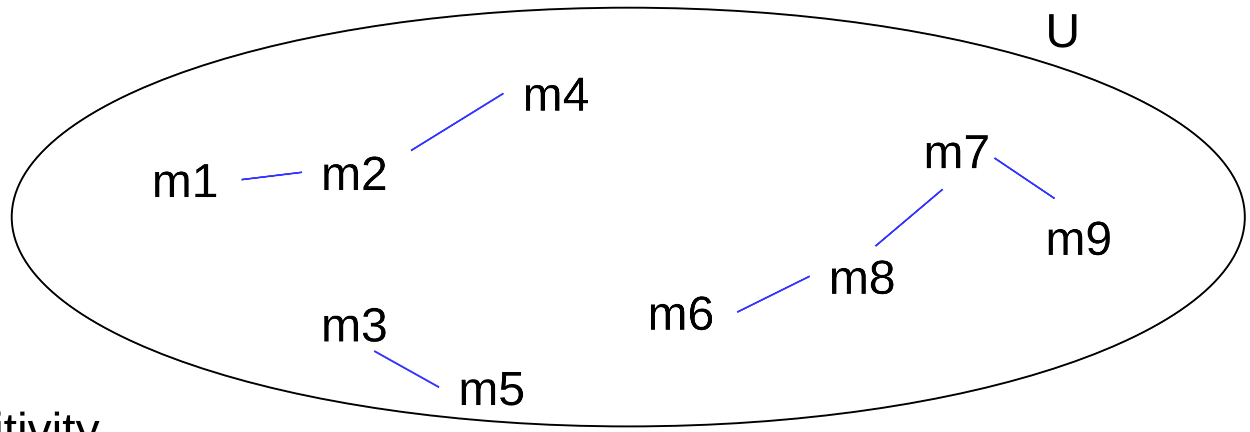



by symmetry

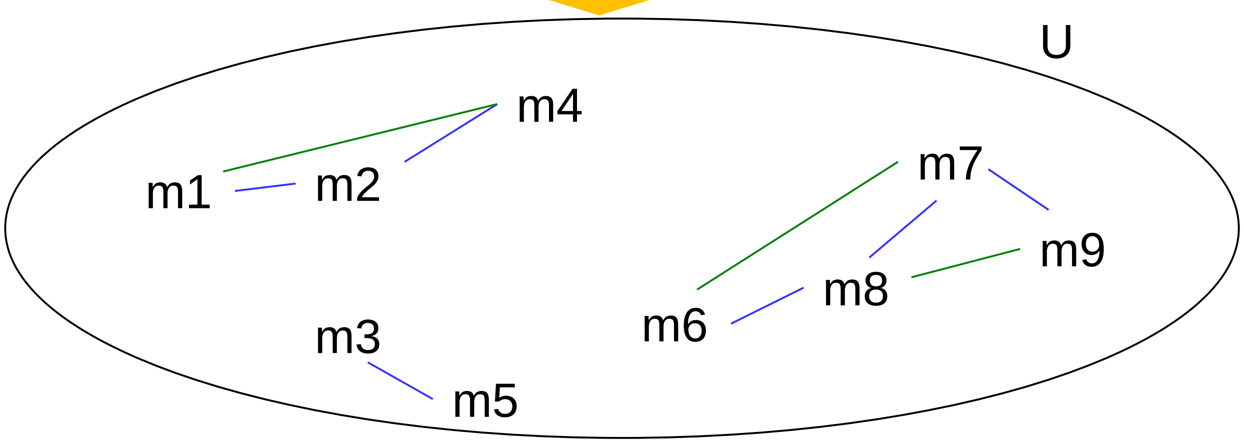


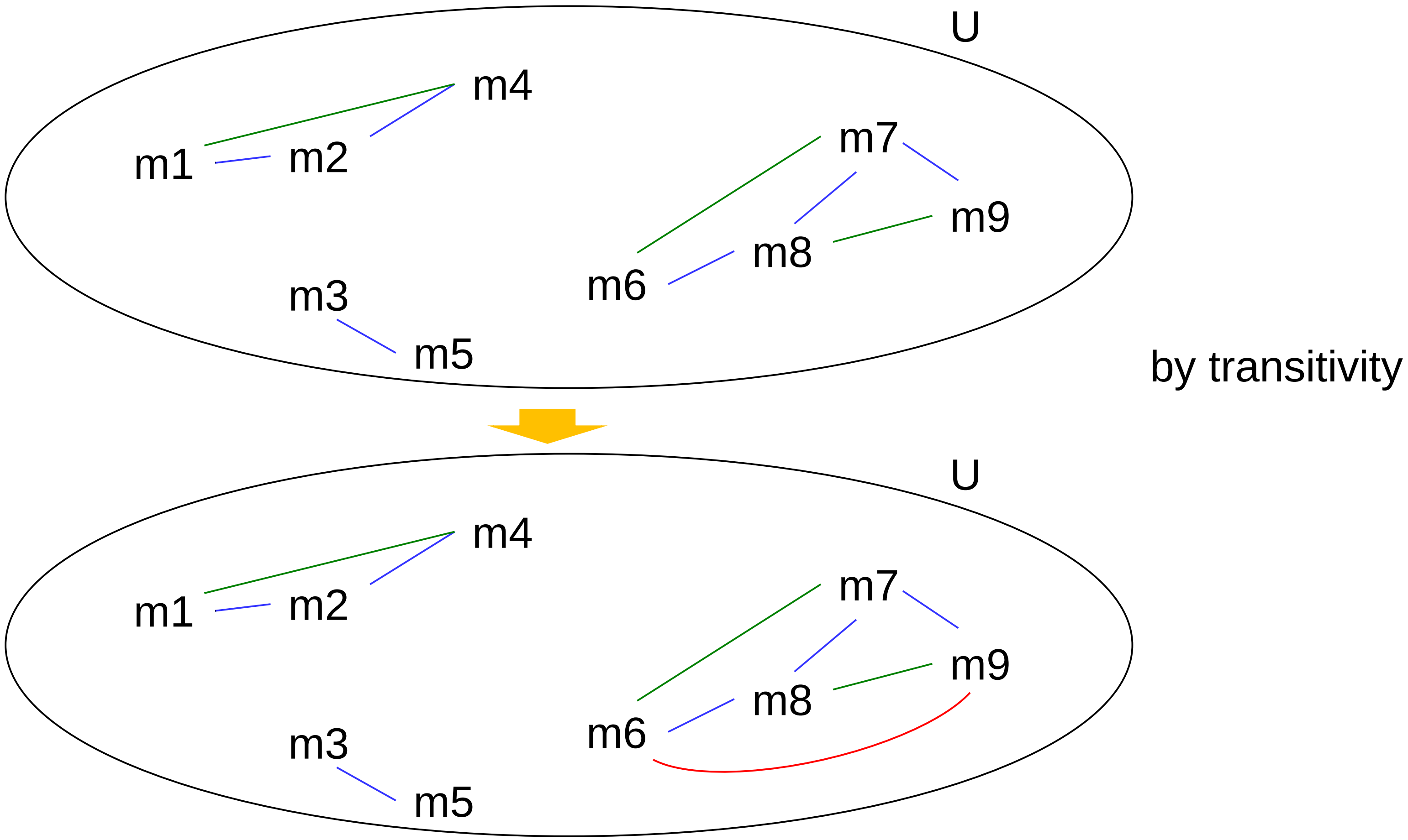


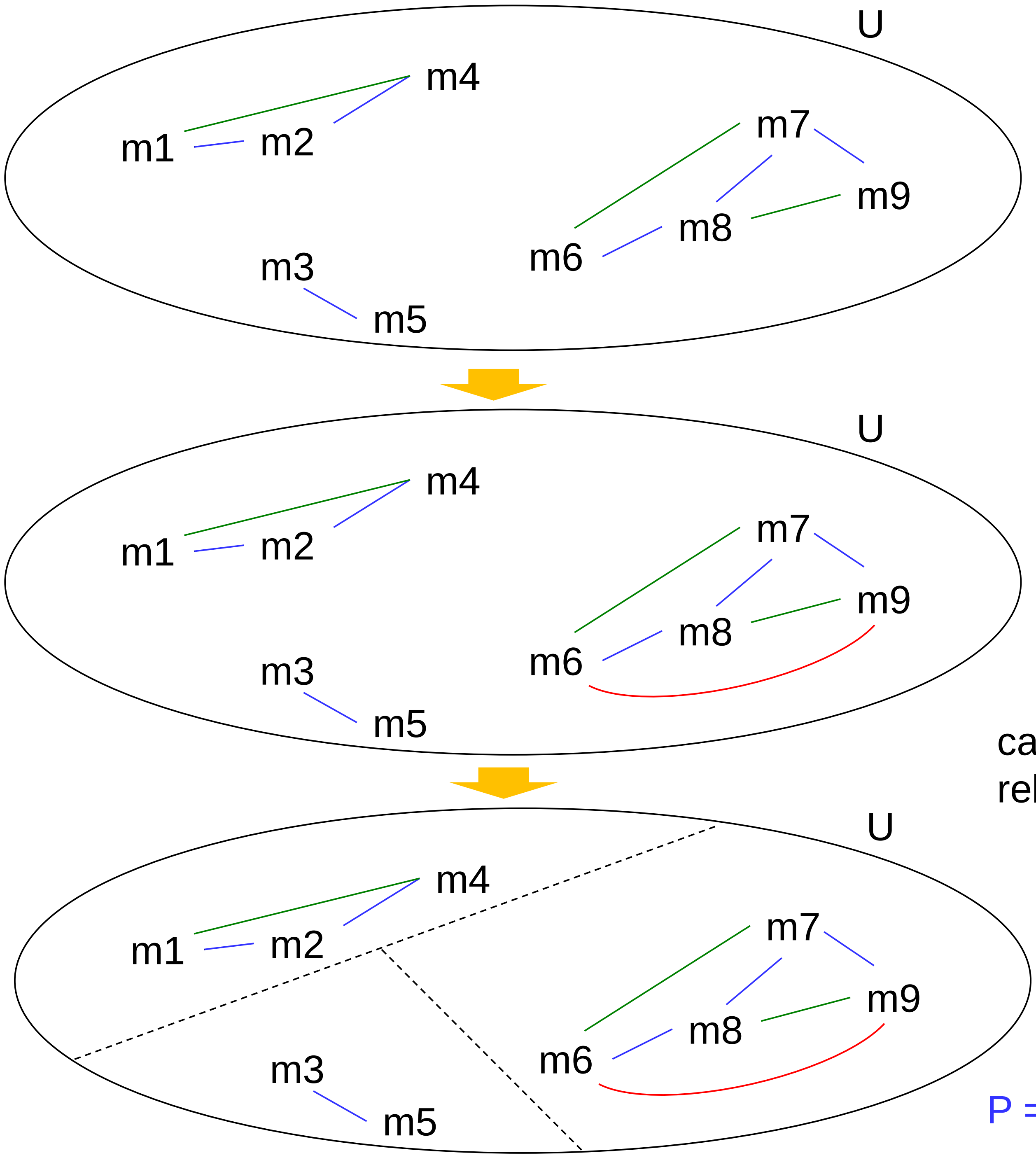

by symmetry




by transitivity




U
m4
m1
m2
m7
m9
m8
m6
m3
m5
by transitivity
U
m4
m1
m2
m7
m9
m8
m6
m3
m5




by transitivity

cannot add any more relationships

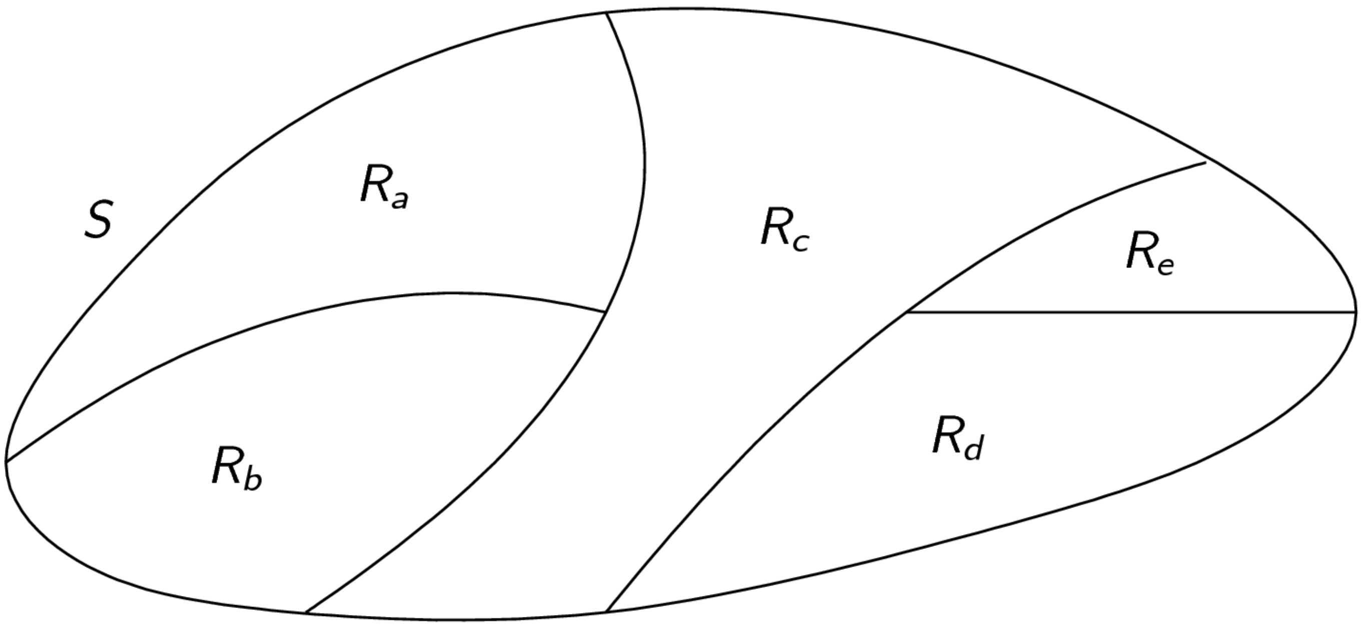
$Likes_{m1}$ = {m1,m2,m4}
$Likes_{m3}$ = {m3, m5}
$Likes_{m6}$ ={m6, m7, m8, m9}

P = {$Likes_{m1}$, $Likes_{m3}$, $Likes_{m6}$}

# Equivalence classes and partitions

## Theorem

*Let $R$ be an equivalence relation on a set $S$. For any element $x \in S$, define $R_x = \{a \in S \mid x\, R\, a\}$, the set of all elements related to $x$. Let $P$ be the collection of distinct subsets of $S$ formed in this way, that is, $P = \{R_x \mid x \in S\}$. Then $P$ is a partition of $S$.*



# Equivalence classes and partitions

**Theorem**

*Let $R$ be an equivalence relation on a set $S$. For any element $x \in S$, define $R_x = \{a \in S \mid x \, R \, a\}$, the set of all elements related to $x$. Let $P$ be the collection of distinct subsets of $S$ formed in this way, that is, $P = \{R_x \mid x \in S\}$. Then $P$ is a partition of $S$.*

Proof)

(1) For any $x \in S$, there is some set $T \in P$ such that $x \in T$. (P is exhaustive.)

(2) If $T1, T2 \in P$ and $T1 \neq T2$, then $T1 \cap T2 = \varnothing$. (P has no overlapping blocks.)

# Equivalence classes and partitions

**Theorem**

*Let $R$ be an equivalence relation on a set $S$. For any element $x \in S$, define $R_x = \{a \in S \mid x\,R\,a\}$, the set of all elements related to $x$. Let $P$ be the collection of distinct subsets of $S$ formed in this way, that is, $P = \{R_x \mid x \in S\}$. Then $P$ is a partition of $S$.*

Proof)

(1) For any $x \in S$, there is some set $T \in P$ such that $x \in T$.

Let $x \in S$. Then since R is reflexive, $xRx$, hence $x \in Rx$.

(2) If $T1, T2 \in P$ and $T1 \neq T2$, then $T1 \cap T2 = \varnothing$.

?

Proof) (2) If $T1, T2 \in P$ and $T1 \neq T2$, then $T1 \cap T2 = \varnothing$.

Suppose $T1, T2 \in P$ and $T1 \neq T2$.

Assume $T1 \cap T2 \neq \varnothing$ for proof by contradiction.

Then there is $x \in T1$ and $x \in T2$.

Then since $xRx$, $x \in Rx$.

To prove $T1 = T2$, we will prove $T1 \subseteq T2$ and $T2 \subseteq T1$.

To show $T1 \subseteq Rx$,

To show $Rx \subseteq T2$,

**Lemma** Let $x,y \in \mathcal{S}$ and $T \in P$ where P is as defined in the Theorem.
Then if $x,y \in T$, then $xRy$ and $yRx$.
Moreover, $x \in Ry$ and $y \in Rx$.

**Example**

R: having the same remainder when divided by 3

$R1 = \{1, 4, 7, 10, 13, ...\}$ $4 \in R1$
$R2 = \{2, 5, 8, 11, 14, ...\}$ $5 \in R2$
$R3 = \{0, 3, 6, 9, 12, ...\}$
$R4 = \{1, 4, 7, 10, 13, ...\}$ $1 \in R3$
$R5 = \{2, 5, 8, 11, 14, ...\}$ $2 \in R5$
. . .

By Lemma,
$11, 23 \in R2$.
So $11R23$ and $23R11$.
Also $11 \in R23$ and $23 \in R11$.
(Actually, $R23 = R11 = R2$ but we will not use this fact.)

Proof) (2) If $T1, T2 \in P$ and $T1 \neq T2$, then $T1 \cap T2 = \varnothing$.
Suppose $T1, T2 \in P$ and $T1 \neq T2$.
Assume $T1 \cap T2 \neq \varnothing$ for proof by contradiction.
Then there is $x \in T1$ and $x \in T2$.
Then since $xRx$, $x \in Rx$.

To show $T1 \subseteq Rx$,
let $y \in T1$. Since $x \in T1$,
both $x \in T1$ and $y \in T1$ are true.
So, by Lemma, $xRy$, hence $y \in Rx$.

To show $Rx \subseteq T2$,
let $y \in Rx$. Then $xRy$.
Since $x \in T2$,
$xRy$ implies $y \in T2$ because
T2 is an equivalence class.

Similarly $T2 \subseteq Rx \subseteq T1$.
So $T1 = T2$.
$\rightarrow\leftarrow$.

Proof) (2) If $T1, T2 \in P$ and $T1 \neq T2$, then $T1 \cap T2 = \varnothing$.

Suppose $T1, T2 \in P$ and $T1 \neq T2$.

Assume $T1 \cap T2 \neq \varnothing$ for proof by contradiction.

Then there is $x \in T1$ and $x \in T2$.

Then since $xRx$, $x \in Rx$.

To show $T1 \subseteq Rx$,

let $y \in T1$. Since $x \in T1$,

both $x \in T1$ and $y \in T1$ are true.

So, by Lemma, $xRy$, hence $y \in Rx$.

To show $Rx \subseteq T2$,

let $y \in Rx$. Then $xRy$.

Since $x \in T2$,

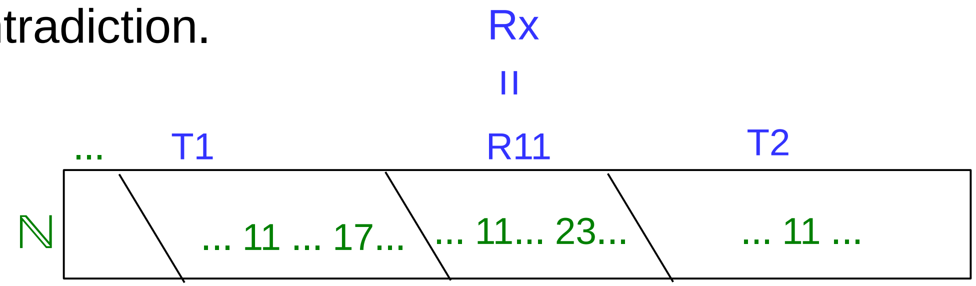
$xRy$ implies $y \in T2$ because

T2 is an equivalence class.

Similarly $T2 \subseteq Rx \subseteq T1$.

So $T1 = T2$.

$\rightarrow\leftarrow$.




$17 \in T1$. Since $11 \in T1$,

both $17 \in T1$ and $17 \in T1$ are true.

So, by Lemma, $11R17$, hence $17 \in R11$.

$23 \in R11$

Then $23R11$.

Since $11 \in T2$,

$23R11$ implies $23 \in T2$ because

T2 is an equivalence class.

$$\begin{array}{r} 365 \\ +\ 217 \\ \hline 582 \end{array}$$

$$\begin{array}{r} 712 \\ \times\ 563 \\ \hline 400856 \end{array}$$

Are these calculations correct?

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 572 \end{array} \qquad\qquad \begin{array}{r} 712 \\ \times\ \ 563 \\ \hline 400856 \end{array}$$

Are these calculations correct?

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 592 \end{array}$$

$\Rightarrow 3+6+5 = 14 \Rightarrow 1+4 = 5$

$\Rightarrow 2+1+7 = 10 \Rightarrow 1+0 = 1$

$+ = 6$

$\Rightarrow \ldots \Rightarrow \ldots = x$

?

$$\begin{array}{r} 365 \\ +\ 217 \\ \hline 582 \end{array}$$

$$\begin{array}{r} 712 \\ \times\ 563 \\ \hline 400856 \end{array}$$

Are these calculations correct?

| | | | | | |
|---|---|---|---|---|---|
| 365 | → | 3+6+5 = 14 | → | 1+4 = 5 | + = 6 |
| + 217 | → | 2+1+7 = 10 | → | 1+0 = 1 | |
| 592 | → | 5+9+2 = 16 | → | 1+6 = 7 | ? |

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 582 \end{array} \qquad\qquad \begin{array}{r} 712 \\ \times\ \ 563 \\ \hline 400856 \end{array}$$

Are these calculations correct?

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 592 \end{array}$$

→ 3+6+5 = 14 → 1+4 = 5

→ 2+1+7 = 10 → 1+0 = 1

+ = 6

→ 5+9+2 = 16 → 1+6 = 7

?

$$\begin{array}{r} 782 \\ \times\ \ 564 \\ \hline 441048 \end{array}$$

→ 7+8+2 = 17 → 1+7 = 8

→ 5+6+4 = 15 → 1+5 = 6

x = 48

→ 4+8=12

→ 1+2= 3

→ 4+4+1+4+8 = 21 → 3

?

Can call this ”abstract computation”.

# Modular arithmetic

Let's read this *equivalence class a*

Fact: Let $[a]$ and $[b]$ be equivalence classes in $\mathbf{Z}/n$. Suppose that $x \in [a]$ and $y \in [b]$. Then $x + y \in [a + b]$ and $xy \in [ab]$.
the operations of addition and multiplication on *equivalence classes* are well-defined:

$$\begin{aligned} [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

This means we can add and multiply elements in $\mathbf{Z}/n$ by adding and multiplying the numbers we use to represent the equivalence class. For example, in the modular arithmetic of $\mathbf{Z}/12$,

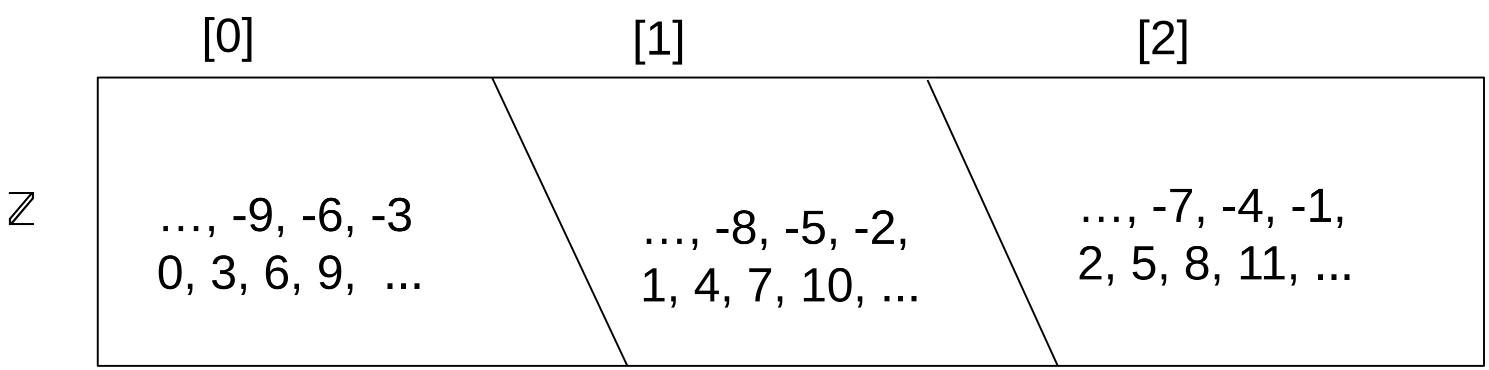
$$[6] + [8] = [2]$$

because $14 \equiv_{12} 2$

# Modular arithmetic

$\mathbb{Z}/3 = \{[0], [1], [2]\}$

where




If $4 \in [1]$ and $5 \in [2]$, then $4+5 \in [9]=[3]=[0]$ and $4 \times 5 \in [20]=[2]$.

# Modular arithmetic

Fact: Let $[a]$ and $[b]$ be equivalence classes in $\mathbf{Z}/n$. Suppose that $x \in [a]$ and $y \in [b]$. Then $x + y \in [a + b]$ and $xy \in [ab]$.

How can we prove this?

To show $x + y \in [a + b]$:

By definition of $\mathbb{Z}/n$, $0 <= a, b < n$. (Can prove $[a-n] = [a]$.)

$x = x1 * n + a$ and $y = y1 * n + b$

$x + y = (x1 + y1) * n + (a+b)$

If $a+b < n$, then $x + y \in [a+b]$.

If $a+b >= n$, then $x + y = [a+b-n]$.

But in this case $[a+b-n] = [a+b]$ .

**Exercise**

Show $xy \in [ab]$:

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 582 \end{array}$$

Is this calculation correct?

$$\begin{array}{r} 365 \\ +\ \ 217 \\ \hline 592 \end{array}$$

$365 \Rightarrow 3+6+5 = 14 \Rightarrow 1+4 \in [5]$

$217 \Rightarrow 2+1+7 = 10 \Rightarrow 1+0 \in [1]$

$+ = [6]$

$592 \Rightarrow 5+9+2 = 16 \Rightarrow 1+6 \in [7]$

**?**

**Why 365∈[5]?**

$$\begin{aligned} 365 &\equiv_9 300 + 60 + 5 \\ &\equiv_9 3\times(99+1) + 6\times(9+1) + 5 \\ &\equiv_9 3\times1 + 6\times1 + 5 \\ &\equiv_9 14 \\ &\equiv_9 1\times(9+1) + 4 \\ &\equiv_9 1+4 \\ &\equiv_9 5 \end{aligned}$$

$$\begin{array}{r} 365 \\ +\quad 217 \\ \hline 582 \end{array}$$

Is this calculation correct?

$$\begin{array}{rcccl} 365 & \Rightarrow & 3+6+5 = 14 & \Rightarrow & 1+4 \in [5] \\ +\quad 217 & \Rightarrow & 2+1+7 = 10 & \Rightarrow & 1+0 \in [1] \\ \hline 592 & \Rightarrow & 5+9+2 = 16 & \Rightarrow & 1+6 \in [7] \end{array} \qquad + = [6]$$

However,

$$\begin{array}{rcccl} 365 & \Rightarrow & 3+6+5 = 14 & \Rightarrow & 1+4 \in [5] \\ +\quad 217 & \Rightarrow & 2+1+7 = 10 & \Rightarrow & 1+0 \in [1] \\ \hline 852 & \Rightarrow & 8+5+2 = 15 & \Rightarrow & 1+5 \in [6] \end{array} \qquad + = [6]$$

That is, this particular checking method does **not guarantee** correctness.

# Quiz 11-2

For the domain $\mathbb{Z}$, which of the following is NOT an equivalence relation?

(a) $\equiv_n$ for $n \in \mathbb{N}^+$

(b) $=$

(c) $\leq \cap \geq$

(d) $\leq \cup \geq$

(e) $\leq \cap =$

(f) The “likes” relation for the domain of weird monkeys.

(g) $< \cup >$