

Logic

- **Statements (Propositions)**

**declarative sentences that are either true or false,
but not both**

Ex. The following are three primitive statements.

**p : Discrete mathematics is a required course
for CS undergraduates.**

**q : Professor Chen teaches discrete
mathematics.**

r : $2 + 3 = 5$.

**Ex. “What a beautiful bird !” and “Get up and do
your exercises.” are not statements, because
they do not have *truth values* (true or false).**

- **Non-primitive Statements**

- ♣ **Negation**

$\neg p$ (not p):

Discrete mathematics is NOT a required course for CS undergraduates.

- ♣ **Conjunction**

$p \wedge q$ (p and q):

Discrete mathematics is a required course for CS undergraduates AND Professor Chen teaches discrete mathematics.

- ♣ **Disjunction**

$p \vee q$ (p or q):

Discrete mathematics is a required course for CS undergraduates OR Professor Chen teaches discrete mathematics.

♣ Implication

$p \rightarrow q$ (p implies q):

IF discrete mathematics is a required
course for CS undergraduates, THEN
Professor Chen teaches discrete
mathematics.

(p is called *hypothesis*; q is called *conclusion*.)

“ $p \rightarrow q$ ” is read “if p , then q ” or

“ p is a **sufficient** condition for q ” or

“ q is a **necessary** condition for p ” or

“ p only if q ”.

p (一個數字能被4整除) ,
是 q (成為偶數) 的充分 (但不必要) 條件。
能被2整除, 則是充分及必要條件。

♣ **Biconditional**

$p \leftrightarrow q$ (p if and only if q):

**Discrete mathematics is a required course
for CS undergraduates IF AND ONLY IF
Professor Chen teaches discrete
mathematics.**

Often, “ p if and only if q ” is abbreviated to
“ p iff q ”.

“ $p \leftrightarrow q$ ” is also read “ p is a *necessary and
sufficient condition* for q .”

“ \wedge ”, “ \vee ”, “ \rightarrow ”, and “ \leftrightarrow ” are referred to as
logical connectives, which combine two or more
statements into a *compound* statement.

- **Truth Tables**

p	$\neg p$
0	1
1	0

0 : false

1 : true

p	q	$p \wedge q$	$p \vee q$	$p \underline{\vee} q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

“ $p \underline{\vee} q$ ” denotes “ p or q in the exclusive sense”.

It is often expressed as “ p XOR q ”.

Ex. The following three implications are true.

♦ If $2 + 3 = 5$, then $2 + 4 = 6$.

♦ If $2 + 3 = 6$, then $2 + 4 = 6$.

♦ If $2 + 3 = 6$, then $2 + 4 = 9$.

But, the following implication is false.

♦ If $2 + 3 = 5$, then $2 + 4 = 7$.

Ex. Pythagorean theorem can be expressed as $p \rightarrow q$,
where

p : A, B , and C are three vertices of a triangle
and the angle A is right;

$$q: \overline{BC}^2 = \overline{AB}^2 + \overline{AC}^2.$$

Ex. p : Discrete mathematics is a required course for CS undergraduates;

q : Professor Chen teaches discrete mathematics;

r : Not all CS undergraduates pass discrete mathematics.

Then,

$\neg r \rightarrow p$:

If all CS undergraduates pass discrete mathematics, then discrete mathematics is a required course for CS undergraduates;

$q \wedge (\neg r \rightarrow p)$:

Professor Chen teaches discrete mathematics and if all CS undergraduates pass discrete mathematics, then discrete mathematics is a required course for CS undergraduates.

p	q	r	$\neg r$	$\neg r \rightarrow p$	$q \wedge (\neg r \rightarrow p)$
0	0	0	1	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	0	1	1
1	0	0	1	1	0
1	0	1	0	1	0
1	1	0	1	1	1
1	1	1	0	1	1

- **Logical Equivalence**

Two statements s_1, s_2 are *logically equivalent*, denoted by $s_1 \Leftrightarrow s_2$, when s_1 is true if and only if s_2 is true.

Ex. $p \rightarrow q \Leftrightarrow \neg p \vee q$.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Ex. $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$p \leftrightarrow q$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

Ex. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q;$

$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q.$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
0	0	0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	1	0	0
1	0	0	1	0	1	1	1	0	0
1	1	1	0	0	0	0	1	0	0

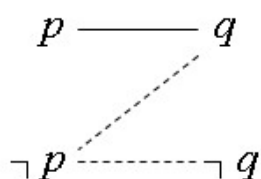
Ex. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r);$

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r).$

p	q	r	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$	$(p \vee q) \wedge (p \vee r)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	1
1	0	0	0	0	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Ex. $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p.$

p	q	$p \rightarrow q$	$\neg q \rightarrow \neg p$	$q \rightarrow p$	$\neg p \rightarrow \neg q$
0	0	1	1	1	1
0	1	1	1	0	0
1	0	0	0	1	1
1	1	1	1	1	1



老子《道德經》 道可道，非常道；名可名，非常名

\Leftrightarrow 常道，不可道；常名，不可名

Other logical equivalences:

◆ $\neg\neg p \Leftrightarrow p$

◆ $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ and

$$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$$

◆ $p \wedge p \Leftrightarrow p$ and $p \vee p \Leftrightarrow p$

◆ $p \wedge T \Leftrightarrow p$, $p \wedge F \Leftrightarrow F$, $p \vee T \Leftrightarrow T$, and

$$p \vee F \Leftrightarrow p$$

◆ $p \wedge \neg p \Leftrightarrow F$ and $p \vee \neg p \Leftrightarrow T$

◆ $p \wedge (p \vee q) \Leftrightarrow p$ and $p \vee (p \wedge q) \Leftrightarrow p$

If $s_1 \Leftrightarrow s_2$ and $s_2 \Leftrightarrow s_3$, then $s_1 \Leftrightarrow s_3$.

Ex. $(p \vee q) \wedge \neg(\neg p \wedge q)$

$$\Leftrightarrow (p \vee q) \wedge (p \vee \neg q)$$

$$\Leftrightarrow p \vee (q \wedge \neg q)$$

$$\Leftrightarrow p \vee F$$

$$\Leftrightarrow p$$

Therefore, $(p \vee q) \wedge \neg(\neg p \wedge q)$ can be simplified to p .

Ex. $\neg(\neg((p \vee q) \wedge r) \vee \neg q)$

$$\Leftrightarrow ((p \vee q) \wedge r) \wedge q$$

$$\Leftrightarrow (p \vee q) \wedge q \wedge r$$

$$\Leftrightarrow ((p \vee q) \wedge q) \wedge r$$

$$\Leftrightarrow q \wedge r \quad (\because (p \vee q) \wedge q \Leftrightarrow q)$$

- **Proof Based on $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$**

Ex. Prove that if $x+y > 100$, then $x > 50$ or $y > 50$.

It is equivalent to prove that if $x \leq 50$ and $y \leq 50$, then $x+y \leq 100$.

Ex. Suppose that n is an integer. Prove that if n^2 is odd, then n is odd.

It is equivalent to prove that if n is even, then n^2 is even.

• Proof by Contradiction

Ex. Prove that if n is the sum of the squares of two odd integers, then n is not a perfect square.

Suppose that n is the sum of the squares of two odd integers and n is a perfect square.

That is, $n = (2x + 1)^2 + (2y + 1)^2$ and $n = z^2$ for some integers x, y, z .

The left equality implies $n = 4(x^2 + y^2 + x + y) + 2$, which is an even number (but not a multiple of 4).

\Rightarrow $z = 2s$ for some integer s .

\Rightarrow $n = z^2$ is a multiple of 4

\Rightarrow a contradiction to $n = 4(x^2 + y^2 + x + y) + 2$

Let $p: n = (2x+1)^2 + (2y+1)^2$;

$q: n \neq z^2$.

The proof for $p \rightarrow q$ true above is based on the following arguments.

1. $p \rightarrow q \Leftrightarrow \neg p \vee q \Leftrightarrow \neg(p \wedge \neg q)$.
2. $p \wedge \neg q$ is false, because it derives a contradiction.

Relations

- **Definition**

r -tuple : (a_1, a_2, \dots, a_r)

- a_i : i -th coordinate (component)
- ordered sequence
- any two coordinates are not necessarily distinct

Cartesian Product :

$$A_1 \times A_2 \times \dots \times A_r = \{(a_1, a_2, \dots, a_r) \mid a_i \in A_i \text{ for } 1 \leq i \leq r\}$$

- A_i : set
- $A_1 \times A_2 \times \dots \times A_r = A^r$, if $A_1 = A_2 = \dots = A_r = A$

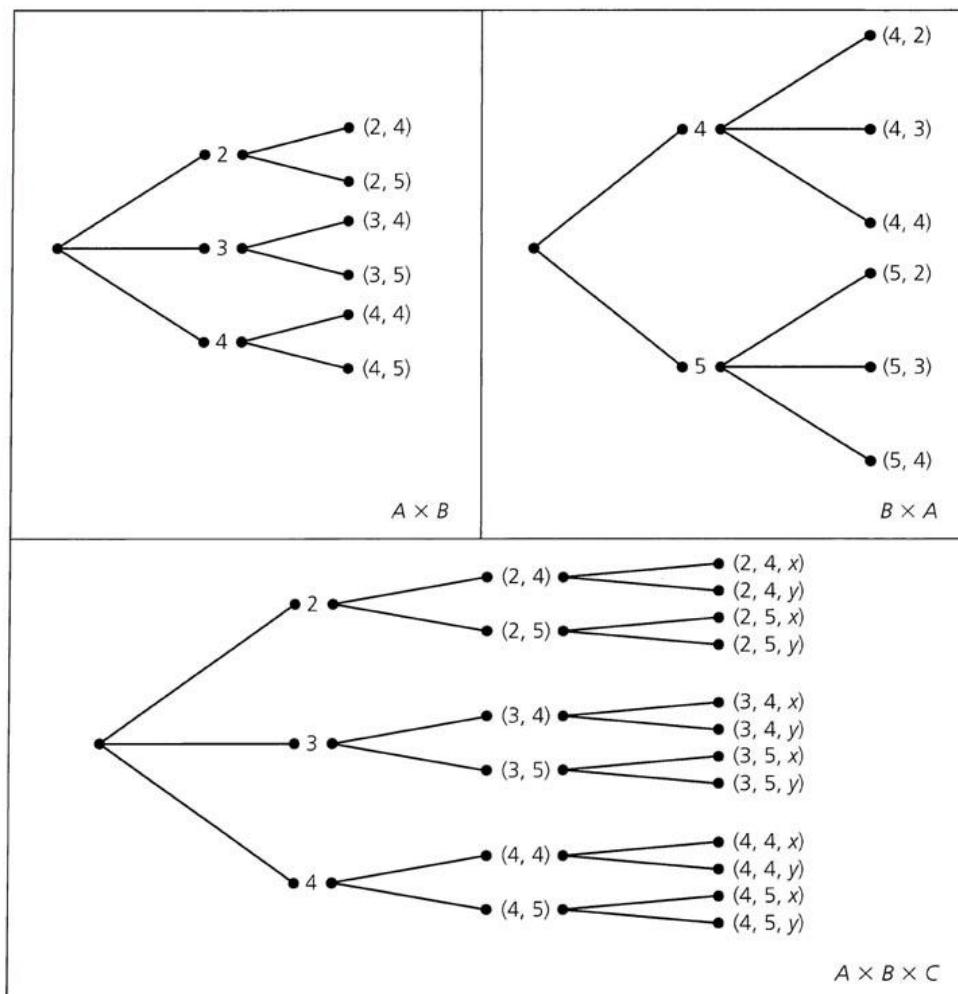
Ex. $A = \{0, 1\}$, $B = \{a, b\}$.

$$A \times B = \{(0, a), (0, b), (1, a), (1, b)\}.$$

$$A^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Tree representation of Cartesian products :

$A = \{2, 3, 4\}$, $B = \{4, 5\}$, and $C = \{x, y\}$.



For any sets A , B , and C ,

$$A \times \emptyset = \emptyset \times A = \emptyset;$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C);$$

$$(A \cap B) \times C = (A \times C) \cap (B \times C);$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C);$$

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

Proof of $A \times (B \cap C) = (A \times B) \cap (A \times C)$:

$$(p, q) \in A \times (B \cap C)$$

$$\Leftrightarrow p \in A \text{ and } q \in B \cap C$$

$$\Leftrightarrow (p \in A, q \in B) \text{ and } (p \in A, q \in C)$$

$$\Leftrightarrow (p, q) \in A \times B \text{ and } (p, q) \in A \times C$$

$$\Leftrightarrow (p, q) \in (A \times B) \cap (A \times C)$$

Relation : A subset of $A_1 \times A_2 \times \dots \times A_r$ is called an *r-ary relation* on A_1, A_2, \dots, A_r .

- there are $2^{|A_1| \times |A_2| \times \dots \times |A_r|}$ relations on A_1, A_2, \dots, A_r

Ex. Suppose $A = \{2, 3, 4\}$ and $B = \{4, 5\}$. The following are some relations from A to B .

\emptyset , $\{(2, 4)\}$, $\{(2, 4), (2, 5)\}$, $\{(2, 4), (3, 4), (4, 4)\}$,
 $\{(2, 4), (3, 4), (4, 5)\}$, and $A \times B$.

But, $\{(4, 2)\}$, $\{(2, 4), (5, 3)\}$, and $\{(2, 5), (3, 3), (4, 4)\}$
are not.

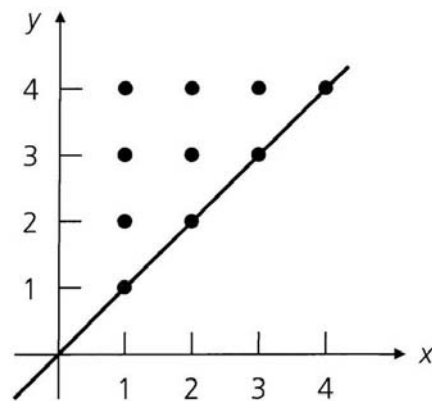
Ex. $A = \{2, 3, 4\}$ and $B = \{2, 3, 4, 5, 6\}$.

A relation R on A, B is defined as follows :

$a R b$ iff a divides b .

$\Rightarrow R = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$.

Ex. Suppose $A = \mathbb{Z}^+$. We define a binary relation R on A (from A to A) as follows: $x R y$ iff $x \leq y$. When (x, y) is regarded as a point in the Euclidean plane, R is the set of points located on or above the line $y = x$.



Ex. Define R on Z as follows: $x R y$ iff $x - y$ is a multiple of 7.

Then, $(9, 2), (-3, 11), (14, 0) \in R$, but $(3, 7) \notin R$.

Ex. Suppose $S = \{1, 2, 3, 4, 5, 6, 7\}$ and $C = \{1, 2, 3, 6\}$.

Define R on the power set of S as follows: $A R B$ iff $A \cap C = B \cap C$.

Then, $(\{4, 5\}, \{7\}), (\{1, 2, 4, 5\}, \{1, 2, 5, 7\}) \in R$,
but $(\{1, 2, 3, 4, 5\}, \{1, 2, 3, 6, 7\}) \notin R$.

$$\begin{array}{c} A \quad B \\ \{4, 5\} \cap C = \emptyset \\ \{7\} \cap C = \emptyset \end{array}$$

• Binary Relations

Representation of a binary relation :

$$R = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}.$$

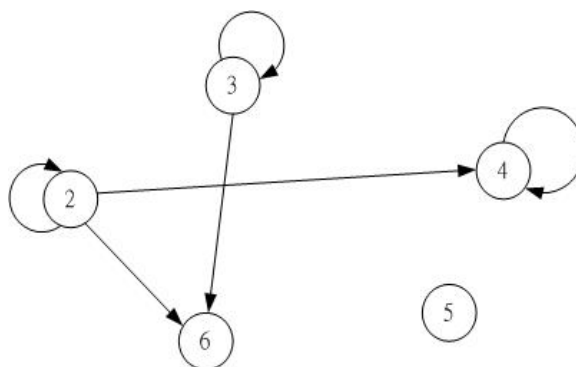
1. Relation matrix

$$\begin{array}{c} \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{array}{c} 2 \\ 3 \\ 4 \end{array} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

$$A = \{2, 3, 4\}$$

$$B = \{2, 3, 4, 5, 6\}$$

2. Graph representation



R : a binary relation on A (i.e., from A to A).

- R is **reflexive** iff $\forall x \in A (x R x)$.

Ex. “=” and “ \supseteq ” are reflexive.

自己 = 自己

- R is **irreflexive** iff $\forall x \in A (x \not R x)$.

Ex. “ \subset ” and “ $<$ ” are irreflexive.

- R is **symmetric** iff $\forall x, y \in A (x R y \Rightarrow y R x)$.

Ex. “=” is symmetric.

- R is **asymmetric** iff $\forall x, y \in A (x R y \Rightarrow y \not R x)$.

Ex. “ $<$ ” is asymmetric.

- R is **antisymmetric** iff $\forall x, y \in A (x R y \text{ and } y R x \Rightarrow x = y)$.

Ex. “ \leq ” and “ \subseteq ” are antisymmetric.

- R is **transitive** iff $\forall x, y, z \in A (x R y \text{ and } y R z \Rightarrow x R z)$.

Ex. “=” is transitive.

Ex. The following are some binary relations on $A = \{1, 2, 3, 4\}$.

$$R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}.$$

$$R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1)\}.$$

$$R_3 = \{(1, 2), (2, 1), (3, 4), (4, 3)\}.$$

$$R_4 = \{(1, 2), (1, 3), (2, 3), (3, 4)\}.$$

$$R_5 = \{(1, 1), (2, 2), (2, 3), (3, 4), (2, 4)\}.$$

reflexive : R_1, R_2

irreflexive : R_3, R_4

symmetric : R_1, R_2, R_3

asymmetric : R_4

antisymmetric : R_1, R_4, R_5

transitive : R_1, R_2, R_5

Ex. Define R to be a binary relation on the set of integers, where $a R b$ iff $ab \geq 0$.

R is reflexive and symmetric.

R is not transitive.

(for example, $-5 R 0$, $0 R 8$, but $-5 \not R 8$)

Suppose $A = \{1, 2, \dots, n\}$.

1. There are 2^{n^2-n} reflexive binary relations on A .

Each reflexive binary relation on A must contain $(1, 1), (2, 2), \dots, (n, n)$.

$$|A \times A - \{(i, i) : 1 \leq i \leq n\}| = n^2 - n.$$

2. There are $2^{(n^2+n)/2}$ symmetric binary relations on A .

$$A \times A = \{(i, i) : 1 \leq i \leq n\} + \{(i, j) : 1 \leq i \leq n, 1 \leq j \leq n, \text{ and } i \neq j\}.$$

$$\underline{2^n \times 2^{(n^2-n)/2} = 2^{(n^2+n)/2}}.$$

n : diagonal entries

$(n^2 - n) / 2$: 右上三角 (或左下) : $1 + \dots + (n - 1) = [1 + (n - 1)](n - 1) / 2$

3. There are $2^{(n^2-n)/2}$ reflexive and symmetric binary relations on A .

$$1 + \dots + (n - 1) = (n^2 - n) / 2$$

4. There are $2^n \times 3^{(n^2-n)/2}$ antisymmetric binary relations on A .

Each (i, i) can be either included or excluded.

For each pair of (i, j) and (j, i) , there are three choices:

(a) include (i, j) and exclude (j, i) ;

(b) exclude (i, j) and include (j, i) ;

(c) exclude (i, j) and (j, i) .

$\Rightarrow 2^n \times 3^{(n^2-n)/2}$.

~~include (i, j) and (j, i)~~
 $i \neq j$

5. There is no general formula for counting the number of transitive binary relations on A .

R_1 : a relation from A_1 to A_2

R_2 : a relation from A_2 to A_3 .

The *composition* of R_1 and R_2 , denoted by $R_1 \circ R_2$, is a relation from A_1 to A_3 .

$$R_1 \circ R_2 = \{(x, y) \mid x R_1 z \text{ and } z R_2 y \text{ for some } z \in A_2\}.$$

Ex. $R_1 = \{(1, 2), (3, 4), (2, 4), (4, 2)\}$.

$$R_2 = \{(2, 4), (2, 3), (4, 1)\}.$$

$$R_1 \circ R_2 = \{(1, 4), (1, 3), (3, 1), (2, 1), (4, 4), (4, 3)\}.$$

Generally, $\overbrace{R \circ R \circ \dots \circ R}^k$ is written as R^k .

Intuitively, if $(x, y) \in R^k$, there is a path (or cycle as $x=y$) of length k from x to y in the graph representation of R .

R^0 : the *identity relation*, i.e., $\{(x, x) \mid x \in A\}$.

$R^+ = \bigcup_{i=1}^{\infty} R^i$ is called the *transitive closure* of R .

$R^* = R^0 \cup R^+$ is called the *reflexive transitive closure* of R .

- $R^+ = R \circ R^* = R^* \circ R$.
- $R = R^+$ if R is transitive.
- $R = R^*$ if R is both reflexive and transitive.
- If R is a binary relation on A , then $R^+ = \bigcup_{i=1}^{|A|} R^i$.

(It is interesting to find R^+ only when R is not transitive.)

$$\begin{aligned}
R \circ R^* &= R \circ (R^0 \cup R^+) \\
&= (R \circ R^0) \cup (R \circ R^+) \\
&= R \cup \bigcup_{i=2}^{\infty} R^i \\
&= \bigcup_{i=1}^{\infty} R^i \\
&= R^+
\end{aligned}$$

$$\begin{aligned}
R \text{ is transitive} &\Rightarrow R^2 = R \circ R \subseteq R \\
&R^3 = R^2 \circ R \subseteq R \\
&\vdots \\
&R^{|A|} = R^{|A|-1} \circ R \subseteq R \\
&\Rightarrow R^+ = R
\end{aligned}$$

• Equivalence Relations

A binary relation R on A is an *equivalence relation* iff it is **reflexive**, **symmetric** and **transitive**.

Ex. “=” is an equivalence relation.

Ex. The relation R defined below is an equivalence relation.

	1	2	3	4
1	1	1	0	0
2	1	1	0	0
3	0	0	1	1
4	0	0	1	1

{1, 2} and {3, 4} are called equivalence classes.

Let R be an equivalence relation on A .

A subset E of A is an *equivalence class* with respect to R and A iff

1. $\forall x, y \in E \ (x R y)$;
2. $\forall x \in E, \forall y \in A - E \ (x \not R y)$.

A method to construct equivalence classes :

Ex. $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (3, 6),$
 $(4, 3), (4, 4), (4, 6), (5, 5), (6, 3), (6, 4), (6, 6)\}.$

Initially : $\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}$

Scan R :

$(1, 2) \in R$ $\{1, 2\}, \{3\}, \{4\}, \{5\}, \{6\}$

$(3, 4) \in R$ $\{1, 2\}, \{3, 4\}, \{5\}, \{6\}$

$(3, 6) \in R$ $\{1, 2\}, \{3, 4, 6\}, \{5\}$

The set of equivalence classes with respect to R and A forms a partition of A .

$(\{S_1, S_2, \dots, S_k\}$ is a *partition* of A iff $\bigcup_{i=1}^k S_i = A$ and

$S_i \cap S_j = \emptyset$ for all $i \neq j$.)

Ex. Define R on the set Z of integers as follows:

$$a R b \text{ iff } 4 \text{ divides } a - b.$$

R is an equivalence relation, and its equivalence classes, denoted by $[0]$, $[1]$, $[2]$ and $[3]$, are as follows:

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\} = \{4k \mid k \in Z\};$$

$$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\} = \{4k + 1 \mid k \in Z\};$$

$$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\} = \{4k + 2 \mid k \in Z\};$$

$$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\} = \{4k + 3 \mid k \in Z\}.$$

Ex. Define R on the set Z of integers as follows:

$$a R b \text{ iff } a^2 = b^2.$$


R is an equivalence relation, and its equivalence classes are $\{0\}$, $\{-1, 1\}$, $\{-2, 2\}$, \dots , $\{-i, i\}$, \dots .

Ex. Suppose that R is an equivalence relation on $\{1, 2, \dots, 7\}$, and the induced partition is $\{\{1, 2\}, \{3\}, \{4, 5, 7\}, \{6\}\}$.

Then, $R = \{(1, 1), (2, 2), (1, 2), (2, 1)\} \cup \{(3, 3)\} \cup \{(4, 4), (5, 5), (7, 7), (4, 5), (5, 4), (4, 7), (7, 4), (5, 7), (7, 5)\} \cup \{(6, 6)\}$.

There is a one-to-one correspondence between the set of equivalence relations on $\{1, 2, \dots, n\}$ and the set of partitions of $\{1, 2, \dots, n\}$.

 **Ex. What is the number of equivalence relations on $A = \{1, 2, \dots, 6\}$?**

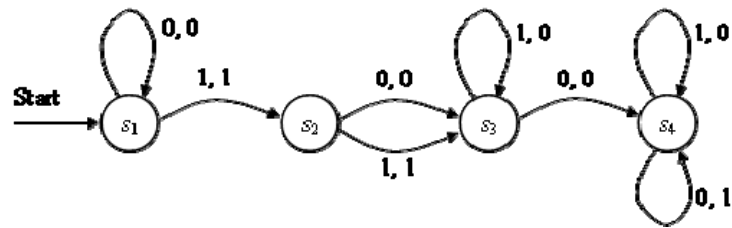
 **Let $f(m)$ be the number of onto functions from A to $B = \{b_1, b_2, \dots, b_m\}$ (m is the number of equivalence classes), which can be evaluated by the principle of inclusion and exclusion or exponential generating functions (refer to page 80 in "Combinatorics").**

The answer is equal to

$$\begin{aligned} & f(1) + f(2)/2! + f(3)/3! + f(4)/4! + f(5)/5! + f(6)/6! \\ &= 1 + 31 + 90 + 65 + 15 + 1 \\ &= 203. \end{aligned}$$

**Ex. An application in the minimization process of
finite state machines (FSMs)**

an FSM



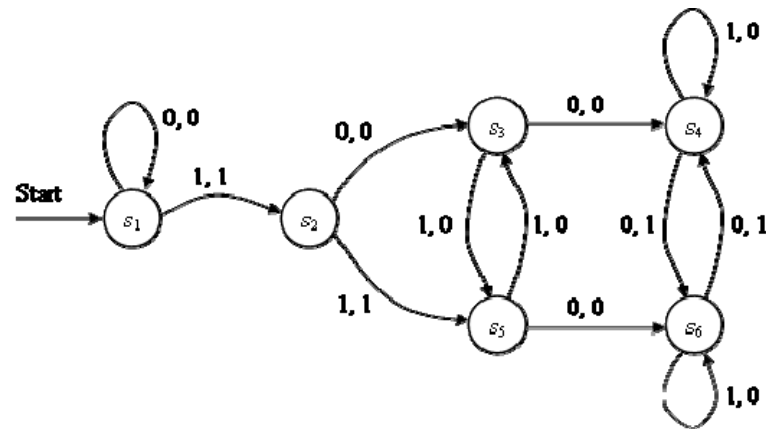
input string : 010010

output string : 010001

state transition :

$s_1 \Rightarrow s_1 \Rightarrow s_2 \Rightarrow s_3 \Rightarrow s_4 \Rightarrow s_4 \Rightarrow s_4$

another FSM



input string : 010010 (the same as above)

output string : 010001 (the same as above)

state transition :

$$s_1 \Rightarrow s_1 \Rightarrow s_2 \Rightarrow s_3 \Rightarrow s_4 \Rightarrow s_4 \Rightarrow s_6$$

In fact, the two FSMs are equivalent, with respect to the output string, because they always generate the same output string for any input string.

The second FSM contains some redundant states (e.g., $\{s_3, s_5\}$ and $\{s_4, s_6\}$). The redundant states can be replaced with a single state without changing the function of the FSM.

The minimization process can transform an FSM with redundant states into another FSM without redundant states.

An FSM can be represented by a state table.

**The following is the state table of the second FSM,
where ν denotes a state transition function and ω
denotes an output function.**

	ν		ω	
	0	1	0	1
s_1	s_1	s_2	0	1
s_2	s_3	s_5	0	1
s_3	s_4	s_5	0	0
s_4	s_6	s_4	1	0
s_5	s_6	s_3	0	0
s_6	s_4	s_6	1	0

The minimization process is described below.

Step 1. Partition the set of states so that s_i and s_j belong to the same subset if and only if $\omega(s_i, 0) = \omega(s_j, 0)$ and $\omega(s_i, 1) = \omega(s_j, 1)$.

$$P_1 = \{\{s_1, s_2\}, \{s_3, s_5\}, \{s_4, s_6\}\}.$$

Step 2. Partition each subset obtained in Step 1 so that s_i and s_j get together if and only if $\nu(s_i, x)$ and $\nu(s_j, x)$ fall into the same subset of the current partition, where $x \in \{0, 1\}$.

$$\{s_1, s_2\} \rightarrow \{\{s_1\}, \{s_2\}\};$$

$$\{s_3, s_5\} \rightarrow \{\{s_3, s_5\}\};$$

- $\{s_4, s_6\} \rightarrow \{\{s_4, s_6\}\}.$

$$\Rightarrow P_2 = \{\{s_1\}, \{s_2\}, \{s_3, s_5\}, \{s_4, s_6\}\}.$$

Step 3. Repeat Step 2 until no further partition is possible (i.e., $P_k = P_{k-1}$ for some $k \geq 2$).

For this example, P_2 is the final partition.

Step 4. Keep one state in each subset of the final partition, and eliminate the others.

After elimination, we have, for example,

$$P_2 = \{\{s_1\}, \{s_2\}, \{s_3\}, \{s_4\}\},$$

and the resulting FSM is identical with the first FSM.

Define an equivalence relation R as follows:

$s_i R s_j$ if and only if $\omega(s_i, I) = \omega(s_j, I)$ for any input string I .

The minimization process is first to partition the set of states with respect to R , and then further partition each subset according to the function ν . Finally, the states in the same subset are redundant to one another.

The concept of FSM was widely used in

- software design (e.g., compiler design),**
 - logic circuit design,**
 - probability analysis (e.g., Markov model),**
- to name a few.**

• Partial Ordering, Total Ordering

Partial ordering : a relation on A is called a **partial ordering** if it is **reflexive**, **anti-symmetric** and **transitive**, where A is called a **partially ordered set** (*poset* for short).

A partial ordering is commonly denoted by \preceq .

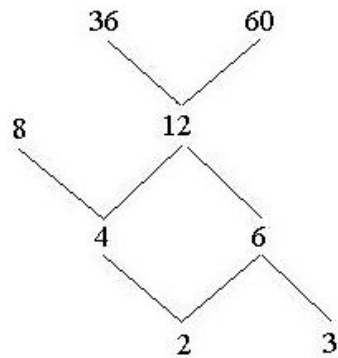
Ex. “ \geq ”, “ \leq ”, “ \subseteq ” and “ \supseteq ” are partial orderings.

$$x R x$$
$$x R y, y R x, x = y$$

When A is finite, a partial ordering on A can be conveniently represented by an ordering diagram, called *Hasse diagram*.

- Each element is a vertex.
- A vertex a_i appears below another vertex a_j ($a_i \neq a_j$) iff $a_i \preceq a_j$.
- An edge connects a_i with a_j iff $a_i \preceq a_j$ and there is no a_k such that $a_i \preceq a_k \preceq a_j$.

Ex. $A = \{2, 3, 4, 6, 8, 12, 36, 60\}$. A partial ordering defined on A is : $i \mid j$ iff i is a divisor of j .



minimal elements : 2, 3

maximal elements : 8, 36, 60

upper (lower) bound of 4, 6 : 12, 36, 60 (2)

least (greatest) upper (lower) bound of 4, 6 : 12 (2)

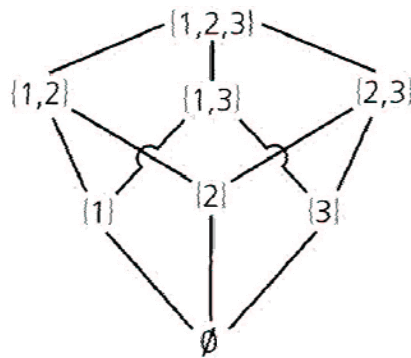
A poset A is called a **lattice**, if every two elements of A have upper bounds and lower bounds in A .

partial order set

Ex. The **poset** A in the above example is not a lattice.

Ex. Let A be the power set of $\{1, 2, 3\}$.

Define R on A as follows: $a R b$ iff $a \subset b$.



($\{1, 2, 3\}$ is called the *greatest* element, and \emptyset is call the *least* element.)

The least upper bound (greatest lower bound) of a and b is $a \cup b$ ($a \cap b$).

$\Rightarrow A$ is a lattice

If we “stretch” the ordering diagram in such a way that all vertices are aligned in a single column, with all descending paths preserved, we get a *topological order* of the elements of A .

(It is possible that there are multiple topological orders for a poset.)

60	60	36	36
36	8	60	60
12	36	12	8
8	12	6	12
4	6	3	4
6	4	8	6
3	2	4	2
2	3	2	3

The elements a_1, a_2, \dots, a_n (e.g., 60, 36, 12, 8, 4, 6, 3, 2) of a poset A are in a topological order iff there exists no $1 \leq j < i \leq n$ with $a_j \preceq a_i$.

Total ordering : a partial ordering \preceq on A is called a
total ordering if for all $a_i, a_j \in A$,
either $a_i \preceq a_j$ or $a_j \preceq a_i$.

Ex. “ \leq ” and “ \geq ” are total ordering.

The ordering diagram for a total ordering is a chain.



(do Exercise #5)

Boolean Algebra

• Definition

K : a set of elements

$+, \cdot$: two binary operators

$(K, \cdot, +)$ is a *Boolean algebra* iff the following holds:

1. Closure under \cdot and $+$

For all $a, b \in K$, $a \cdot b \in K$ and $a + b \in K$.

2. Commutativity of \cdot and $+$

For all $a, b \in K$, $a \cdot b = b \cdot a$ and $a + b = b + a$.

3. Distributivity of \cdot and $+$

For all $a, b, c \in K$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and

$a + (b \cdot c) = (a + b) \cdot (a + c)$.

4. Identity and zero elements

K contains two elements 1 (*identity*) and 0 (*zero*) :

$$a \cdot 1 = a \text{ and } a + 0 = a \text{ for all } a \in K.$$

5. Complement

For every $a \in K$, there exists \bar{a} ($\neq a$) such that

$$a \cdot \bar{a} = 0 \text{ and } a + \bar{a} = 1.$$

\bar{a} is the *complement* of a .

6. There are at least two distinct elements a and b ($a \neq b$) in K .

Ex. ($\{true, false\}, \wedge, \vee$) is a Boolean algebra.

- 1. Distributivity may be verified by the truth table method (refer to page 11).**
- 2. The identity and zero are *true* and *false*, respectively.**

Ex. Let $K = \{1, 2, 3, 5, 6, 10, 15, 30\}$ be the set of all positive integer divisors of 30. For any $a, b \in K$, define $a + b$ ($a \cdot b$) to be the l.c.m. (g.c.d.) of a, b , and $\bar{a} = 30/a$. Then, with 1 as the zero and 30 as the identity, $(K, \cdot, +)$ is a Boolean algebra.

Proof of $a + (b \cdot c) = (a + b) \cdot (a + c)$:

Let $a = 2^{k_1} 3^{k_2} 5^{k_3}$, $b = 2^{m_1} 3^{m_2} 5^{m_3}$, $c = 2^{n_1} 3^{n_2} 5^{n_3}$.

Then $b \cdot c = 2^{s_1} 3^{s_2} 5^{s_3}$, where $s_i = \min\{m_i, n_i\}$. So,

$a + (b \cdot c) = 2^{t_1} 3^{t_2} 5^{t_3}$, where $t_i = \max\{k_i, \min\{m_i, n_i\}\}$.

Also, $(a + b) \cdot (a + c) = 2^{u_1} 3^{u_2} 5^{u_3}$, where $u_i = \min\{\max\{k_i, m_i\}, \max\{k_i, n_i\}\}$. Since k_i, m_i and n_i are all either 0 or 1, we have $t_i = u_i$.

Let α and β be two Boolean expressions. α and β are said to be *duals* of each other, if one can be derived from the other by using the following substitution.

1. Replace all occurrences of \cdot by $+$ and $+$ by \cdot .
2. Replace all occurrences of 0 by 1 and 1 by 0.

Ex. $a + b$ and $a \cdot b$ are duals of each other.

**$(a \cdot b \cdot c) + (c \cdot d) + (a \cdot f)$ and $(a + b + c) \cdot (c + d) \cdot (a + f)$
are duals of each other.**

Notice that dual Boolean expressions appear in the definitions of closure, commutativity, distributivity, identity, zero and complement.

Theorem. (Principle of Duality) If S is a theorem about a Boolean algebra, and S can be proved with closure, commutativity, distributivity, identity, zero, complement and some properties derived from them, then its dual is likewise a theorem.

Ex. Proof of $x + x = x$, where $(K, \cdot, +)$ is a Boolean algebra and $x \in K$.

$x = x + 0$	zero
$= x + (x \cdot \bar{x})$	complement
$= (x + x) \cdot (x + \bar{x})$	distributivity
$= (x + x) \cdot 1$	complement
$= x + x$	identity

Proof of $x \cdot x = x$

$x = x \cdot 1$	identity
$= x \cdot (x + \bar{x})$	complement
$= (x \cdot x) + (x \cdot \bar{x})$	distributivity
$= (x \cdot x) + 0$	complement
$= x \cdot x$	zero

Theorem. Let $(K, \cdot, +)$ be a Boolean algebra.

- (1) *The identity and zero are unique.*
- (2) *$a \cdot a = a$ and $a + a = a$ for every $a \in K$.*
- (3) *$a \cdot 0 = 0$ and $a + 1 = 1$ for every $a \in K$.*
- (4) *\bar{a} is unique for every $a \in K$.*
- (5) *$\overline{(\bar{a})} = a$ for every $a \in K$.*
- (6) *The identity and zero are distinct. Also, $\bar{1} = 0$ and $\bar{0} = 1$.*
- (7) *$a \cdot (a + b) = a$ and $a + (a \cdot b) = a$ for every $a, b \in K$ (absorption law).*
- (8) *$a \cdot b = a \cdot c$ and $\bar{a} \cdot b = \bar{a} \cdot c \Rightarrow b = c$.
 $a + b = a + c$ and $\bar{a} + b = \bar{a} + c \Rightarrow b = c$.*
- (9) *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ and $a + (b + c) = (a + b) + c$ for every $a, b, c \in K$.*
- (10) *$\overline{a \cdot b} = \bar{a} + \bar{b}$ and $\overline{a + b} = \bar{a} \cdot \bar{b}$ for every $a, b \in K$ (DeMorgan's law).*

Proof. (1) Suppose 1 and 1' are two identities.

$$1 = 1' \cdot 1 = 1'.$$

$$\begin{aligned} (3) \quad a \cdot 0 &= (a \cdot 0) + 0 \\ &= (a \cdot 0) + (a \cdot \bar{a}) \\ &= a \cdot (0 + \bar{a}) \\ &= a \cdot \bar{a} \\ &= 0. \end{aligned}$$

(4) Suppose \bar{a} and \bar{a}' are complements of a .

$$\begin{aligned} \bar{a} \cdot \bar{a}' &= \bar{a} \cdot \bar{a}' + 0 = (\bar{a} \cdot \bar{a}') + (\bar{a} \cdot a) \\ &= \bar{a} \cdot (\bar{a}' + a) = \bar{a} \cdot 1 = \bar{a}. \end{aligned}$$

Similarly, $\bar{a}' \cdot \bar{a} = \bar{a}'$.

Thus, $\bar{a} = \bar{a}'$.

(5) An immediate consequence of the definition of complement (refer to page 56).

(6) If $K = \{0, 1\}$, then $0 \neq 1$ by definition.

If $|K| > 2$, then select $a \notin \{0, 1\}$.

Suppose conversely $1 = 0$.

$$\Rightarrow a + 1 = a + 0$$

$$\Rightarrow 1 = a, \text{ a contradiction}$$

$$\bar{1} = \bar{1} \cdot 1 = 0.$$

$$\begin{aligned} (7) \quad a \cdot (a + b) &= (a \cdot a) + (a \cdot b) = a + (a \cdot b) \\ &= (a \cdot 1) + (a \cdot b) = a \cdot (1 + b) = a \cdot 1 \\ &= a. \end{aligned}$$

$$(8) \quad b = 1 \cdot b = (a + \bar{a}) \cdot b = (a \cdot b) + (\bar{a} \cdot b)$$

$$c = 1 \cdot c = (a + \bar{a}) \cdot c = (a \cdot c) + (\bar{a} \cdot c)$$

$$\Rightarrow b = c, \text{ if } a \cdot b = a \cdot c \text{ and } \bar{a} \cdot b = \bar{a} \cdot c$$

$$\begin{aligned}
(9) \quad a + (a \cdot (b \cdot c)) &= (a + a) \cdot (a + (b \cdot c)) \\
&= a \cdot (a + (b \cdot c)) = a.
\end{aligned}$$

$$\begin{aligned}
a + ((a \cdot b) \cdot c) &= (a + (a \cdot b)) \cdot (a + c) \\
&= a \cdot (a + c) = a.
\end{aligned}$$

$$\begin{aligned}
\text{Similarly, } \bar{a} + (a \cdot (b \cdot c)) &= \bar{a} + ((a \cdot b) \cdot c) \\
&= \bar{a} + (b \cdot c).
\end{aligned}$$

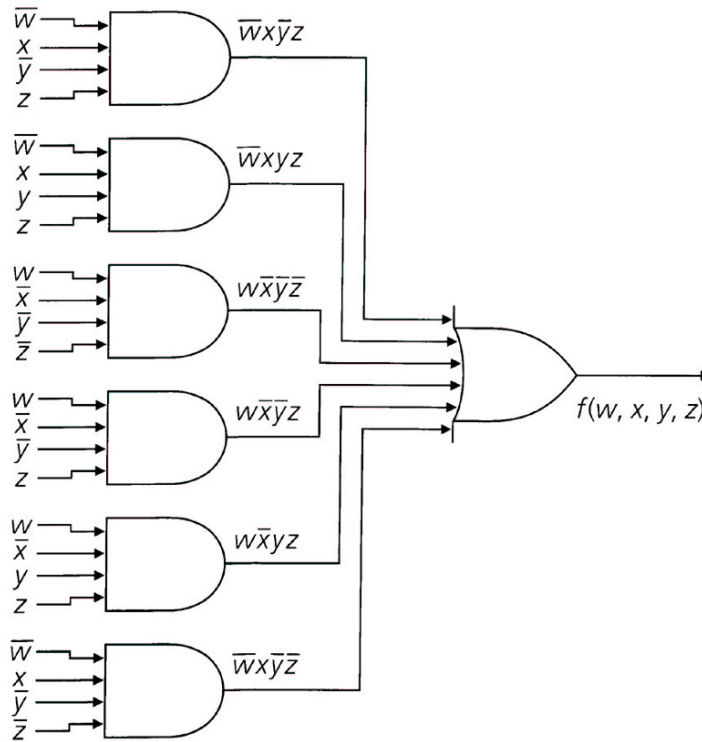
Thus, from (8), $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

$$\begin{aligned}
(10) \quad (a \cdot b) + (\bar{a} + \bar{b}) &= ((a \cdot b) + \bar{a}) + \bar{b} \\
&= ((a + \bar{a}) \cdot (b + \bar{a})) + \bar{b} = (1 \cdot (b + \bar{a})) + \bar{b} \\
&= (b + \bar{a}) + \bar{b} = (\bar{a} + b) + \bar{b} = \bar{a} + (b + \bar{b}) \\
&= \bar{a} + 1 = 1.
\end{aligned}$$

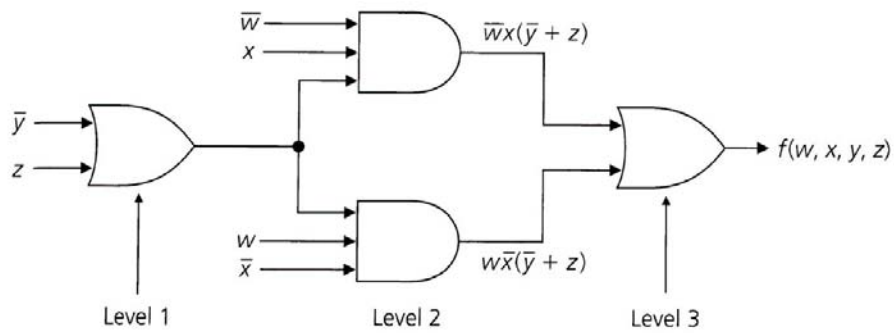
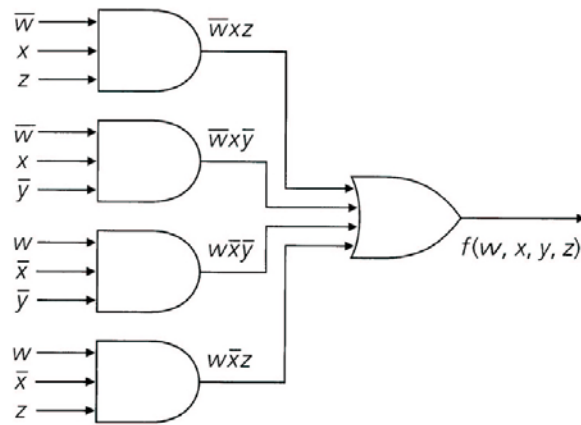
$$\begin{aligned}
(a \cdot b) \cdot (\bar{a} + \bar{b}) &= ((a \cdot b) \cdot \bar{a}) + ((a \cdot b) \cdot \bar{b}) \\
&= (b \cdot (a \cdot \bar{a})) + (a \cdot (b \cdot \bar{b})) = 0 + 0 = 0.
\end{aligned}$$

Thus, $\bar{a} + \bar{b}$ is the complement of $a \cdot b$.

$$f(w, x, y, z) = \overline{w}x\overline{y}z + \overline{w}xyz + w\overline{x}\overline{y}z + w\overline{x}yz + \overline{w}x\overline{y}\overline{z} + \overline{w}x\overline{y}z$$



$$\begin{aligned}
f(w, x, y, z) &= \overline{w}xz(\overline{y} + y) + w\overline{x}\overline{y}(\overline{z} + z) + w\overline{x}yz + \\
&\quad \overline{w}x\overline{y}z \\
&= \overline{w}xz + \overline{w}x\overline{y} + w\overline{x}yz + \overline{w}x\overline{y}z \\
&= \overline{w}x(z + \overline{y}z) + w\overline{x}(\overline{y} + yz) \\
&= \overline{w}x(z(1 + \overline{y}) + \overline{y}z) + w\overline{x}(\overline{y}(1 + z) + yz) \\
&= \overline{w}x(z + \overline{y}(z + \overline{z})) + w\overline{x}(\overline{y} + z(\overline{y} + y)) \\
&= \overline{w}x(z + \overline{y}) + w\overline{x}(\overline{y} + z) \\
&= \overline{w}xz + \overline{w}x\overline{y} + w\overline{x}\overline{y} + w\overline{x}z
\end{aligned}$$



The elements of a finite Boolean algebra can be partially ordered.

Suppose that $(K, \cdot, +)$ is a Boolean algebra.

For $a, b \in K$, define $a \preceq b$ iff $a \cdot b = a$.

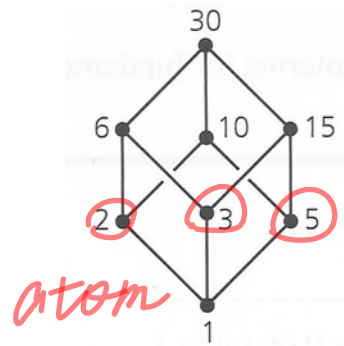
Then, \preceq is a partial ordering.

reflexive: $a \cdot a = a \Rightarrow a \preceq a$.

antisymmetric: $a \preceq b, b \preceq a \Rightarrow a \cdot b = a, b \cdot a = b$
 $\Rightarrow a = b$.

transitive: $a \preceq b, b \preceq c \Rightarrow a \cdot b = a, b \cdot c = b$
 $\Rightarrow a = a \cdot b = a \cdot (b \cdot c) = (a \cdot b) \cdot c$
 $= a \cdot c$
 $\Rightarrow a \preceq c$.

The Hasse diagrams for the Boolean algebra of page 51 is depicted below.



Notice that $0 \preceq a$, $a \preceq 1$ for every $a \in K$.

($0 = 1$ and $1 = 30$ for the example above)

A nonzero element $a \in K$ is called an **atom** of K , if $b \preceq a$ implies $b = 0$ or $b = a$, where $b \in K$.

For the example above, the Boolean algebra has three atoms: 2, 3, 5.

台灣大學

The following four facts are proved in pages 738-739 of Grimaldi's book.

Fact 1. If a is an atom of K , then $a \cdot b = 0$ or $a \cdot b = a$ for every $b \in K$.

(Since $(a \cdot b) \cdot a = a \cdot (b \cdot a) = a \cdot (a \cdot b) = (a \cdot a) \cdot b = a \cdot b$, we have $a \cdot b \preceq a$. Then, Fact 1 follows.)

Fact 2. If $a_1 \neq a_2$ are two atoms of K , then $a_1 \cdot a_2 = 0$.

(By Fact 1, a_1 is an atom $\Rightarrow a_1 \cdot a_2 \in \{0, a_1\}$.

Also, a_2 is an atom $\Rightarrow a_2 \cdot a_1 \in \{0, a_2\}$.

Since $a_1 \neq a_2$, Fact 2 follows.)

Fact 3. Suppose that a_1, a_2, \dots, a_n are atoms of K , and b is a nonzero element in K . Without loss of generality, assume $b \cdot a_i \neq 0$ for $1 \leq i \leq k$, and $b \cdot a_i = 0$ for $k+1 \leq i \leq n$. Then, $b = a_1 + a_2 + \dots + a_k$.

For the example above, we have $10 = 2 + 5$ and $30 = 2 + 3 + 5$.

Fact 4. If K has n atoms, then $|K| = 2^n$.

Suppose that a_1, a_2, \dots, a_n are the n atoms of K .

There is a one-to-one correspondence between K

and $\left\{ \sum_{i=1}^n c_i \cdot a_i : c_i = 0, 1 \text{ for } 1 \leq i \leq n \right\}$.

For the example above, $|K| = 2^3 = 8$.

Rings

• Definition

R : a set of distinct elements

$+, \cdot$: two binary operators

$(R, +, \cdot)$ is a *ring* if for all $a, b, c \in R$, the following are satisfied :

1. Closure under $+$ and \cdot

$$a + b \in R, \quad a \cdot b \in R$$

2. Associativity of $+$ and \cdot

$$a + (b + c) = (a + b) + c$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. Commutativity of $+$

$$a + b = b + a$$

4. Identity for $+$

**There exists $z \in R$ such that $a + z = z + a = a$
for every $a \in R$.**

5. Inverse under $+$

**For each $a \in R$, there exists $b \in R$ with
 $a + b = b + a = z$.**

6. Distributivity of \cdot over $+$

$$**$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$**$$

$$**$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$**$$

Ex. Under ordinary addition and multiplication, \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} are rings. Their additive identity is 0 , and the additive inverse of x is $-x$.

The identity z for $+$ is often referred to as the *zero* of the ring.

Let $(R, +, \cdot)$ be a ring.

1. If $a \cdot b = b \cdot a$ for all $a, b \in R$, then R is called a *commutative ring*.

2. Suppose $a \neq z$ and $b \neq z$.

If $a \cdot b = z$, then a, b are called *proper divisors of zero* or *proper zero divisors* or *zero divisors* simply.

(“proper” means $a \neq z, b \neq z$.)

R is said to *have no proper divisor of zero* if for

any $a, b \in R$, $a \cdot b = z \Rightarrow a = z$ or $b = z$.

3. If there exists $u \in R$ such that $a \cdot u = u \cdot a = a$ for all $a \in R$, we call u the unity, or *multiplicative identity*, of R . R is then called a *ring with unity*.

Ex. Let $M_2(\mathbb{Z})$ denote the set of all 2×2 matrices with integer components. We define

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix};$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \bullet \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

$(M_2(\mathbb{Z}), +, \bullet)$ is a ring.

(a) additive identity $z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

(b) additive inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

(c) $(M_2(\mathbb{Z}), +, \bullet)$ is not commutative.

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 4 & 7 \end{bmatrix} \neq \begin{bmatrix} 10 & 13 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}.$$

(d) $(M_2(\mathbb{Z}), +, \bullet)$ has proper divisors of zero.

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \bullet \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Let R be a ring with unity u and $a, b \in R$.

If $a \cdot b = b \cdot a = u$, then a, b are *multiplicative inverses* of each other (a, b are also called *units* of R).

Ex. Define two binary operations \oplus, \odot on Z as follows:

$$a \oplus b = a + b - 1, \quad a \odot b = a + b - ab.$$

Then, (Z, \oplus, \odot) is a commutative ring.

Associativity of \oplus and \odot :

$$\begin{aligned} (a \oplus b) \oplus c &= (a + b - 1) \oplus c = (a + b - 1) + c - 1 \\ &= a + b + c - 2 = a + (b + c - 1) - 1 \\ &= a \oplus (b + c - 1) = a \oplus (b \oplus c). \end{aligned}$$

$$\begin{aligned} (a \odot b) \odot c &= (a + b - ab) \odot c \\ &= ((a + b - ab) + c) - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc \\ &= (a + (b + c - bc)) - a(b + c - bc) \\ &= a \odot (b + c - bc) = a \odot (b \odot c). \end{aligned}$$

Identity for \oplus : 1 .

$$a \oplus 1 = a + 1 - 1 = a.$$

Inverse of a under \oplus : $2 - a$.

$$a \oplus (2 - a) = a + (2 - a) - 1 = 1 \text{ (additive identity).}$$

Distributivity of \odot over \oplus :

$$\begin{aligned}
 a \odot (b \oplus c) &= a \odot (b + c - 1) = a + (b + c - 1) - a(b + c - 1) \\
 &= 2a + b + c - ab - ac - 1 \\
 &= ((a + b - ab) + (a + c - ac)) - 1 \\
 &= (a + b - ab) \oplus (a + c - ac) = (a \odot b) \oplus (a \odot c).
 \end{aligned}$$

Similarly, $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$.

In addition, (Z, \oplus, \odot) has a unity 0.

$$a \odot 0 = a + 0 - a \times 0 = a.$$

(Z, \oplus, \odot) has no proper divisor of zero.

$$\begin{aligned}
 a \odot b = 1 &\Leftrightarrow a + b - ab = 1 \Leftrightarrow (a - 1)(1 - b) = 0 \\
 &\Leftrightarrow a = 1 \text{ or } b = 1.
 \end{aligned}$$

2 has a multiplicative inverse 2, because $2 \odot 2 =$

$2 + 2 - 2 \times 2 = 0$, but 3 has no multiplicative inverse

(if c is the multiplicative inverse 3, then $3 \odot c =$

$3 + c - 3c = 0$, which implies $c = 3/2 \notin Z$).

Ex. Let $R = \{a, b, c, d, e\}$, and define $+$ and \cdot as follows.

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

\cdot	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

$(R, +, \cdot)$ is a commutative ring with unity.

zero : a .

unity : b .

units : b, c, d, e .

Besides, $(R, +, \cdot)$ has two properties:

- (1) no proper divisors of zero (thus called an integral domain);
- (2) a multiplicative inverse for every nonzero element (thus called a field).

- **Integral Domain**

Let R be a ring. Then, R is an *integral domain* if the following hold.

1. R is commutative.

2. R has a unity u ($u \neq z$).

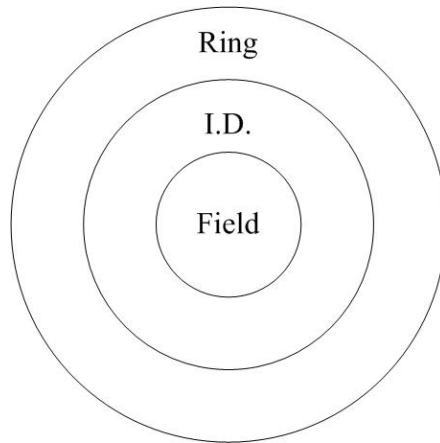
($u \neq z$ means that an integral domain has at least two elements.)

3. R has no zero divisor.

• Field

Let R be a ring. Then R is a *field* if the following holds.

1. R is commutative.
2. R has a unity u ($u \neq z$).
3. There is a multiplicative inverse of a ($\neq z$) for every $a \in R$.



1. a multiplicative inverse of a ($\neq z$) for every $a \in R$

\Rightarrow the cancellation law of multiplication

(not necessarily true reversely)

2. the cancellation law of multiplication

\Leftrightarrow no zero divisor

Ex. Under ordinary addition and multiplication,

Z is an integral domain, but not a field, and

Q, R, C are both integral domains and fields.

Ex. The ring in the example of p. 82 is both an

integral domain and a field.

Ex. Let $R = \{s, t, v, w, x, y\}$, and define $+$ and \cdot as follows.

$+$	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

\cdot	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

$(R, +, \cdot)$ is a commutative ring with unity.

zero : s .

unity : t .

units : t, y .

$(R, +, \cdot)$ is not an integral domain, because $v \cdot w = s$.

$(R, +, \cdot)$ is not a field, because v, w and x have no multiplicative inverses.

The cancellation law of multiplication does not hold
because $v \cdot v = v \cdot y = x$.

• Properties of Rings

Theorem. For any ring $(R, +, \cdot)$,

- (a) the zero (additive identity) z is unique;*
- (b) the additive inverse of each $a \in R$ is unique.*

Proof.

- (a)** Let z_1 and z_2 be two zeros. Then,

$$z_1 = z_1 + z_2 = z_2.$$

- (b)** Let b and c be two additive inverses of a .

$$a + b = b + a = z \quad \text{and} \quad a + c = c + a = z.$$

$$\begin{aligned} \text{Then, } b &= b + z = b + (a + c) = (b + a) + c \\ &= z + c = c. \end{aligned}$$

The additive inverse of a is denoted by $-a$.

Theorem. (Cancellation Laws of Addition)

For $a, b, c \in R$,

$$(a) \quad a + b = a + c \Rightarrow b = c ;$$

$$(b) \quad b + a = c + a \Rightarrow b = c.$$

A general ring does not necessarily satisfy the cancellation laws of multiplication.

Theorem. $a \cdot z = z \cdot a = z$ for any $a \in R$.

Proof. $z + a \cdot z = a \cdot z = a \cdot (z + z) = a \cdot z + a \cdot z$

$$\Rightarrow z = a \cdot z.$$

Similarly, $z = z \cdot a$

Theorem. Suppose that $(R, +, \cdot)$ is a ring.

For any $a, b \in R$,

(a) $-(-a) = a$;

(b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;

(c) $(-a) \cdot (-b) = a \cdot b$.

Proof.

(a) $a + (-a) = z$. So, a is the additive inverse of $-a$.

(b) $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot z = z$.

So, $a \cdot (-b)$ is the additive inverse of $a \cdot b$.

Similarly, $(-a) \cdot b$ is the additive inverse of $a \cdot b$.

(c) From (b), $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$.

From (a), $-(-(a \cdot b)) = a \cdot b$.

Theorem. Given a ring $(R, +, \cdot)$,

- (a) if R has a unity, it is unique;***
- (b) if R has a unity and x is a unit of R , the multiplicative inverse of x is unique.***

Proof. Left as an exercise.

The multiplicative inverse (if it exists) of x is denoted by x^{-1} .

Theorem. *Let $(R, +, \cdot)$ be a commutative ring with unity. Then, R is an integral domain if and only if for $a, b, c \in R$ and $a \neq z$,*

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

(Hence, a commutative ring with unity that satisfies the cancellation law of multiplication is an integral domain.)

Proof. Equivalently, we show no zero divisor

\Leftrightarrow the cancellation law of multiplication

(if) Let $a, b \in R$ with $a \cdot b = z$.

If $a \neq z$, then $b = z$ because $a \cdot b = z = a \cdot z$.

So, R has no proper divisor of zero.

(only if) Let $a, b, c \in R$, $a \neq z$, and $a \cdot b = a \cdot c$.

$$a \cdot b = a \cdot c \Rightarrow a \cdot b + (-(a \cdot c)) = z$$

$$\Rightarrow a \cdot (b + (-c)) = z$$

$$\Rightarrow b + (-c) = z$$

$$\Rightarrow b = -(-c) = c$$

The cancellation law of multiplication does not imply the existence of multiplicative inverse.

For example, the integral domain $(\mathbb{Z}, +, \cdot)$ satisfies the cancellation law of multiplication, but contains only two elements, 1 and -1 , which have multiplicative inverses.

Theorem. *If $(R, +, \cdot)$ is a field, then it is an integral domain.*

Proof. Let $a, b \in R$ with $a \cdot b = z$.

If $a \neq z$, then $a^{-1} \in R$.

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot z \Rightarrow u \cdot b = z$$

$$\Rightarrow b = z$$

An integral domain is not necessarily a field.

Theorem. *A finite integral domain $(R, +, \cdot)$ is a field.*

Proof. R is finite $\Rightarrow R = \{d_1, d_2, \dots, d_n\}$, where d_i 's
are all distinct.

Let $a \in R$ and $a \neq z$.

R is an integral domain $\Rightarrow a \cdot d_1, a \cdot d_2, \dots, a \cdot d_n$
are all distinct.

Hence, $\{d_1, d_2, \dots, d_n\} = \{a \cdot d_1, a \cdot d_2, \dots, a \cdot d_n\}$.

$u \in R \Rightarrow u = a \cdot d_k = d_k \cdot a$ for some k
 $\Rightarrow a^{-1} = d_k \in R$.

(do Exercise #6)

• Subring

For a ring $(R, +, \cdot)$, a nonempty subset S of R is said to be a *subring* of R , if $(S, +, \cdot)$ is a ring.

Ex. The set of all even integers is a subring of $(\mathbb{Z}, +, \cdot)$.

In fact, for any $n \in \mathbb{Z}^+$, $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is a subring of $(\mathbb{Z}, +, \cdot)$.

Ex. $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$.

Theorem. *Given a ring $(R, +, \cdot)$, a nonempty subset S of R is a subring of R iff*

- 1. for all $a, b \in S$, $a + b \in S$ and $a \cdot b \in S$;*
- 2. for all $a \in S$, $-a \in S$.*

Proof. S is a ring iff $z \in S$.

$$z = a + (-a) \in S.$$

Ex. Consider the ring (Z, \oplus, \odot) again, where

$$a \oplus b = a + b - 1 \text{ and } a \odot b = a + b - ab$$

for any $a, b \in Z$.

Let $Z_{\text{odd}} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ be the set of odd integers.

Then, $(Z_{\text{odd}}, \oplus, \odot)$ is a subring of (Z, \oplus, \odot) , because

$$(1) \quad a, b \in Z_{\text{odd}} \Rightarrow a \oplus b, a \odot b \in Z_{\text{odd}};$$

$$(2) \quad a \in Z_{\text{odd}} \Rightarrow -a \in Z_{\text{odd}}.$$

(The inverse, i.e., $-a$, of a under \oplus is $2 - a$.)

Theorem. *For any ring $(R, +, \cdot)$, if $S \subseteq R$ and $S \neq \emptyset$, then*

- (1) *$(S, +, \cdot)$ is a subring of R iff for $a, b \in S$,
 $a + (-b) \in S$ and $a \cdot b \in S$;*
- (2) *if S is finite, then $(S, +, \cdot)$ is a subring of R iff
for $a, b \in S$, $a + b \in S$ and $a \cdot b \in S$.*

Proof. (1) • $z \in S$.

$$\text{Let } a = b \Rightarrow b + (-b) = z \in S.$$

- For each $b \in S$, $-b \in S$.

$$\text{Let } a = z \Rightarrow z + (-b) = -b \in S.$$

- $a + b \in S$ for all $a, b \in S$.

$$a, -b \in S \Rightarrow a + (-(-b)) = a + b \in S$$

(2) Assume $S = \{s_1, s_2, \dots, s_n\}$.

For every $a \in S$, $\{a + s_1, a + s_2, \dots, a + s_n\} = S$.

$\Rightarrow a = a + s_k = s_k + a$ for some $1 \leq k \leq n$

$\Rightarrow s_k = z \in S$

$(a + s_k = a = a + z$ assures $s_k = z)$

$\Rightarrow z = a + s_l = s_l + a$ for some $1 \leq l \leq n$

$\Rightarrow s_l = -a \in S$

Ex. Consider the ring $(M_2(\mathbb{Z}), +, \cdot)$.

Let S be the set of 2×2 matrices of the form

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}, \text{ where } x, y \in \mathbb{Z}.$$

Then, $(S, +, \cdot)$ is a subring of $(M_2(\mathbb{Z}), +, \cdot)$, as explained below.

$$\text{Let } \alpha = \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \text{ and } \beta = \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix},$$

where $\alpha, \beta \in S$.

$$\begin{aligned} & \alpha + (-\beta) \\ &= \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} + \begin{bmatrix} -v & -(v+w) \\ -(v+w) & -v \end{bmatrix} \\ &= \begin{bmatrix} x-v & (x-v)+(y-w) \\ (x-v)+(y-w) & x-v \end{bmatrix} \\ &\in S. \end{aligned}$$

$$\alpha \cdot \beta$$

$$= \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \cdot \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix}$$

$$= \begin{bmatrix} 2xv + yv + xw + yw & 2xv + yv + xw \\ 2xv + yv + xw & 2xv + yv + xw + yw \end{bmatrix}$$

$$= \begin{bmatrix} X & X + (-yw) \\ X + (-yw) & X \end{bmatrix}$$

$$\in S,$$

$$\text{where } X = 2xv + yv + xw + yw.$$

- **Ideal**

A subset I of a ring R is an *ideal* of R if the following hold:

1. I is a subring of R ;
2. $x \in I$ and $r \in R$ imply $x \cdot r \in I$ and $r \cdot x \in I$.

Ex. Consider the ring (Z, \oplus, \odot) again, where $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$ for any $a, b \in Z$.

$(Z_{\text{odd}}, \oplus, \odot)$ is a subring of (Z, \oplus, \odot) , where $Z_{\text{odd}} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$.

$(Z_{\text{odd}}, \oplus, \odot)$ is an ideal, because

$$x \in Z_{\text{odd}}, r \in Z \Rightarrow x \odot r = r \odot x \in Z_{\text{odd}}.$$

Ex. $(Z, +, \cdot)$ is a subring, not an ideal, of $(Q, +, \cdot)$, because $7 \in Z$, $1/3 \in Q$, but $7 \cdot 1/3 = 7/3 \notin Z$.

• The Integer Modulo n

Let $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, and $n > 1$. Define $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n .

Ex. $17 \equiv 2 \pmod{5}$; $-7 \equiv -49 \pmod{6}$;
 $11 \equiv -5 \pmod{8}$.

Define $a R b$ iff $a \equiv b \pmod{n}$.

Theorem. R is an equivalence relation on \mathbb{Z} .

Proof. Left as an exercise.

R partitions Z into n equivalence classes as follows.

$$[0] = \{0 + nx \mid x \in Z\} = \{\dots, -2n, -n, 0, n, 2n, \dots\}.$$

$$[1] = \{1 + nx \mid x \in Z\} = \{\dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots\}.$$

$$\begin{array}{ccc} \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \end{array}$$

$$[n-1] = \{(n-1) + nx \mid x \in Z\} = \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}.$$

Let $Z_n = \{[0], [1], [2], \dots, [n-1]\}$.

For $[a], [b] \in Z_n$, define $+$ and \cdot as follows:

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [ab].$$

Ex. For $n = 7$, $[2] + [6] = [8] = [1]$ and

$$[2] \cdot [6] = [12] = [5].$$

***Theorem.* For $n \in \mathbb{Z}^+$ and $n \geq 2$, $(Z_n, +, \cdot)$ is a commutative ring with unity $[1]$.**

Proof. Left as an exercise.

Ex. Z_5 and Z_6 .

$[i]$ is denoted by i

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Z_5

Z_5 is a field, because every nonzero element has a multiplicative inverse.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Z_6

Z_6 is not a field, because $[2]^{-1}, [3]^{-1}, [4]^{-1}$ do not exist.

Z_6 is not an integral domain, because $[2], [3], [4]$ are proper zero divisors of Z_6 .

沒有人跟 2, 3, 4

相乘 = 1 (unity)

Theorem. Z_n is a field iff n is a prime.

Proof. (if) For each integer $0 < a < n$, we have

$$\gcd(a, n) = 1.$$

$$\Rightarrow \text{there exist integers } s, t \text{ with } as + nt = 1$$

$$\Rightarrow as \equiv 1 \pmod{n}$$

$$\Rightarrow [a] \cdot [s] = [as] = [1]$$

$$\Rightarrow [s] = [a]^{-1}.$$

So, Z_n is a field.

(only if) Assume that $n = n_1 n_2$ is not a prime,

where $n_1 > 1$ and $n_2 > 1$.

$$[n_1] \neq [0] \text{ and } [n_2] \neq [0].$$

$$\text{But, } [n_1] \cdot [n_2] = [n_1 n_2] = [n] = [0].$$

So, Z_n is not an integral domain.

$$\Rightarrow Z_n \text{ is not a field.}$$

Theorem. *In Z_n , $[a]$ has a multiplicative inverse (equivalently, $[a]$ is a unit) iff $\gcd(a, n) = 1$.*

Proof. (if) $\gcd(a, n) = 1$

$$\Rightarrow as + nt = 1$$

$$\Rightarrow as \equiv 1 \pmod{n}$$

$$\Rightarrow [a] \cdot [s] = [as] = [1]$$

$$\Rightarrow [s] = [a]^{-1}.$$

(only if) There exists $[b] \in Z_n$ such that

$$[ab] = [a] \cdot [b] = [1] \text{ (i.e., } [b] = [a]^{-1})$$

$$\Rightarrow ab \equiv 1 \pmod{n}$$

$$\Rightarrow ab + nt = 1$$

$$\Rightarrow \gcd(a, n) = 1.$$

For each integer $0 < a < n$,

(1) $\gcd(a, n) = 1 \Leftrightarrow [a]^{-1}$ exists (i.e., $[a]$ is a unit of Z_n);

(2) $\gcd(a, n) > 1 \Leftrightarrow [a]$ is a proper zero divisor of Z_n .

$$\gcd(a, n) = k > 1 \Rightarrow a = kx, n = ky, \gcd(x, y) = 1$$

$$\Rightarrow [a] \cdot [y] = [ay] = [kxy]$$

$$= [xn] = [0],$$

where $[a] \neq [0]$ and $[y] \neq [0]$;

$[a]$ is a proper zero divisor of Z_n

$$\Rightarrow [a] \cdot [b] = [0], \text{ where } [a] \neq [0] \text{ and } [b] \neq [0]$$

$$\Rightarrow [a]^{-1} \text{ does not exist}$$

(if $[a]^{-1}$ exists, then $[b] = [0]$,

a contradiction)

$$\Rightarrow \gcd(a, n) > 1 \text{ (from (1))}$$

Ex. Find $[25]^{-1}$ in Z_{72} ($\gcd(25, 72) = 1$).

$$(-23) \times 25 + 8 \times 72 = 1.$$

$$\Rightarrow (-23) \times 25 \equiv 1 \pmod{72}$$

$$\Rightarrow [-23] \cdot [25] = [(-23) \times 25] = [1] \text{ in } Z_{72}$$

$$\Rightarrow [25]^{-1} = [-23] = [49]$$

Ex. $\gcd(8, 18) = \gcd(2 \times 4, 2 \times 9) = 2$.

$$\Rightarrow [8] \cdot [9] = [0] \text{ in } Z_{18}$$

$$\Rightarrow [8] \text{ is a proper zero divisor of } Z_{18}$$

Ex. Find x so that $25x \equiv 3 \pmod{72}$, i.e.,

$$[x] \cdot [25] = [3] \text{ in } Z_{72}.$$

$$(-23) \times 25 \equiv 1 \pmod{72}$$

$$\Rightarrow [-23] \cdot [25] = [1] \text{ in } Z_{72}$$

$$\Rightarrow [3] \cdot [-23] \cdot [25] = [3] \text{ in } Z_{72}$$

$$\Rightarrow [-69] \cdot [25] = [3] \text{ in } Z_{72}$$

$$\Rightarrow [x] = [-69] = [3] \text{ in } Z_{72}$$

$$\Rightarrow x \in [3] \text{ in } Z_{72}$$

Ex. How many units and how many proper zero divisors are there in Z_{72} ?

The number of units in Z_{72} is equal to the number of integers a such that $0 < a < 72$ and $\gcd(a, 72) = 1$.

The latter can be computed as

$$\phi(72) = \phi(2^3 \times 3^2) = 72 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 24,$$

where $\phi(n)$ is the Euler's phi function (refer to page 19 of the lecture notes for combinatorics).

The number of proper zero divisors in Z_{72} is equal to $71 - 24 = 47$ (exclusive of $[0]$).

In the study of cryptology, we often need to compute $b^e \bmod n$, where b , e , and n are great integers.

Ex. Find x so that $x \equiv 5^{143} \bmod 222$.

Let $E(i) \equiv 5^i \pmod{222}$, where $i \geq 0$ is an integer.

$$\begin{aligned}\Rightarrow E(2i) &\equiv 5^{2i} \pmod{222} \\ &\equiv (5^i \times 5^i) \pmod{222} \\ &\equiv ((5^i \pmod{222}) \times (5^i \pmod{222})) \pmod{222} \\ &\equiv (E(i))^2 \pmod{222}.\end{aligned}$$

$$143 = 2^7 + 2^3 + 2^2 + 2^1 + 2^0.$$

$$\begin{aligned}\Rightarrow E(143) &\equiv 5^{143} \pmod{222} \\ &\equiv 5^{128} \times 5^8 \times 5^4 \times 5^2 \times 5 \pmod{222} \\ &\equiv (E(2^7) \times E(2^3) \times E(2^2) \times E(2^1) \times E(2^0)) \\ &\quad \pmod{222}.\end{aligned}$$

$$E(2^0) \equiv 5 \pmod{222}.$$

$$E(2^1) \equiv (E(2^0))^2 \pmod{222} \equiv 25 \pmod{222}.$$

$$E(2^2) \equiv (E(2^1))^2 \pmod{222} \equiv 181 \pmod{222}.$$

$$E(2^3) \equiv (E(2^2))^2 \pmod{222} \equiv 127 \pmod{222}.$$

$$E(2^4) \equiv (E(2^3))^2 \pmod{222} \equiv 145 \pmod{222}.$$

$$E(2^5) \equiv (E(2^4))^2 \pmod{222} \equiv 157 \pmod{222}.$$

$$E(2^6) \equiv (E(2^5))^2 \pmod{222} \equiv 7 \pmod{222}.$$

$$E(2^7) \equiv (E(2^6))^2 \pmod{222} \equiv 49 \pmod{222}.$$

$$\Rightarrow E(143) \equiv (E(2^7) \times E(2^3) \times E(2^2) \times E(2^1) \times E(2^0)) \pmod{222}$$

$$\equiv (49 \times 127 \times 181 \times 25 \times 5) \pmod{222}$$

$$\equiv ((49 \times 127) \pmod{222}) \times ((181 \times 25 \times 5) \pmod{222}) \pmod{222}$$

$$\equiv 7 \times 203 \pmod{222}$$

$$\equiv 89 \pmod{222}.$$

$$\Rightarrow x \in [89] \text{ in } Z_{222}$$

• The Chinese Remainder Theorem

Given a_i and m_i , $i = 1, 2, \dots, k$, such that

- (1) $m_i \geq 2$ integer for all $1 \leq i \leq k$;
- (2) $0 \leq a_i \leq m_i - 1$ for all $1 \leq i \leq k$;
- (3) $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$,

where $k \geq 2$, find a solution to

$$x \equiv a_i \pmod{m_i} \text{ for all } 1 \leq i \leq k.$$

A solution x can be obtained as follows.

- Compute $M_i = m_1 \dots m_{i-1} m_{i+1} \dots m_k$ for all $1 \leq i \leq k$.
- Find x_i satisfying $M_i x_i \equiv 1 \pmod{m_i}$ for all $1 \leq i \leq k$.
- $x = a_1 M_1 x_1 + a_2 M_2 x_2 + \dots + a_k M_k x_k$.

Each $y \in [x]$ in $Z_{m_1 m_2 \dots m_k}$ is a solution.

A proof can be found in page 702 of Grimaldi's book.

Ex. $x \equiv 14 \pmod{31}$, $x \equiv 16 \pmod{32}$, and $x \equiv 18 \pmod{33}$.

$$(a_1, a_2, a_3) = (14, 16, 18); (m_1, m_2, m_3) = (31, 32, 33);$$

$$(M_1, M_2, M_3) = (1056, 1023, 992).$$

$$M_1 x_1 \equiv 1 \pmod{m_1} \text{ (i.e., } \gcd(x_1, m_1) = 1)$$

$$\Rightarrow [x_1] = [M_1]^{-1} = [1056]^{-1} = [2]^{-1} = [16] \text{ in } Z_{m_1} = Z_{31}.$$

Similarly, $[x_2] = [31]$ in $Z_{m_2} = Z_{32}$ and $[x_3] = [17]$ in $Z_{m_3} = Z_{33}$.

Then, $x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 = 1047504$, and

$[x] = [1047504] = [32688]$ in $Z_{31 \times 32 \times 33} = Z_{32736}$ is the set of solutions.

- **A Cryptosystem Based on the Chinese Remainder Theorem**

(from "A Database Encryption System with Subkeys," *ACM Trans. Database Systems*, vol. 6, no. 2, 1981)

In the last night of 赤壁之戰, 諸葛亮 intended to send messages p_1, p_2, p_3 to 風伯 with the purpose of 借東風, while 周瑜 was the intruder.

(e.g., $(p_1, p_2, p_3) = (2, 1, 5)$)

Step 1: 風神 generated three relatively prime integers m_1, m_2, m_3 (decryption keys).

(e.g., $(m_1, m_2, m_3) = (3, 5, 7)$)

Step 2: 風神 calculated and broadcast e_1, e_2, e_3 (encryption keys), and M as follows.

$$M = m_1 \times m_2 \times m_3.$$

$$(M_1, M_2, M_3) = (M/m_1, M/m_2, M/m_3).$$

$$M_i x_i \equiv 1 \pmod{m_i} \text{ for } i = 1, 2, 3$$

$$e_i = M_i x_i \text{ for } i = 1, 2, 3$$

$$(\text{e.g., } M = 105, (M_1, M_2, M_3) = (35, 21, 15),$$

$$(x_1, x_2, x_3) = (2, 1, 1), (e_1, e_2, e_3) = (70, 21, 15))$$

Step 3: 諸葛亮 calculated and broadcast C (ciphertext),

where $C \equiv (p_1 \times e_1 + p_2 \times e_2 + p_3 \times e_3) \pmod{M}$ and

$$0 \leq C < M.$$

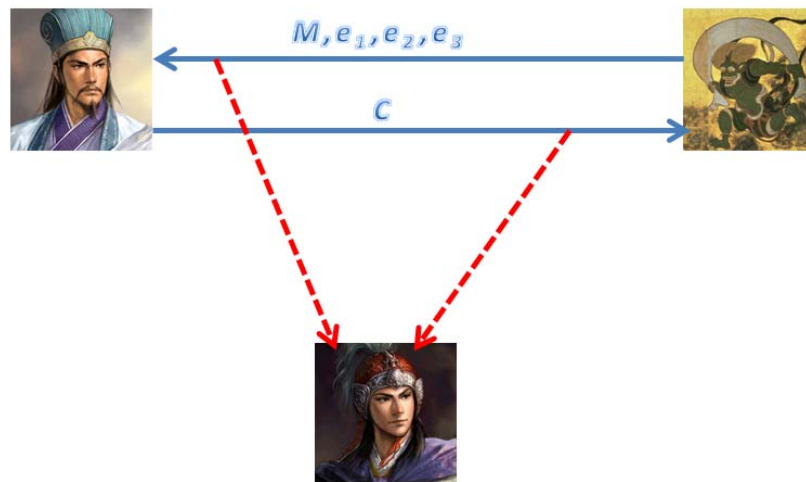
$$(\text{e.g., } C \equiv 236 \pmod{105} \Rightarrow C = 26)$$

Step 4: 風神 got p_1, p_2, p_3 (plaintext) from C , where

$$p_1 \equiv C \pmod{m_1} \quad (26 \pmod{3} \Rightarrow p_1 = 2);$$

$$p_2 \equiv C \pmod{m_2} \quad (26 \pmod{5} \Rightarrow p_2 = 1);$$

$$p_3 \equiv C \pmod{m_3} \quad (26 \pmod{7} \Rightarrow p_3 = 5).$$



Although 周瑜 got encryption keys e_1, e_2, e_3 (and M, C), he was not able to decrypt C for getting p_1, p_2, p_3 unless he also owned decryption keys m_1, m_2, m_3 .

It is extremely time-consuming to obtain m_1, m_2, m_3 from $M (=m_1 \times m_2 \times m_3)$ when M is very large.

• Ring Homomorphism and Isomorphism

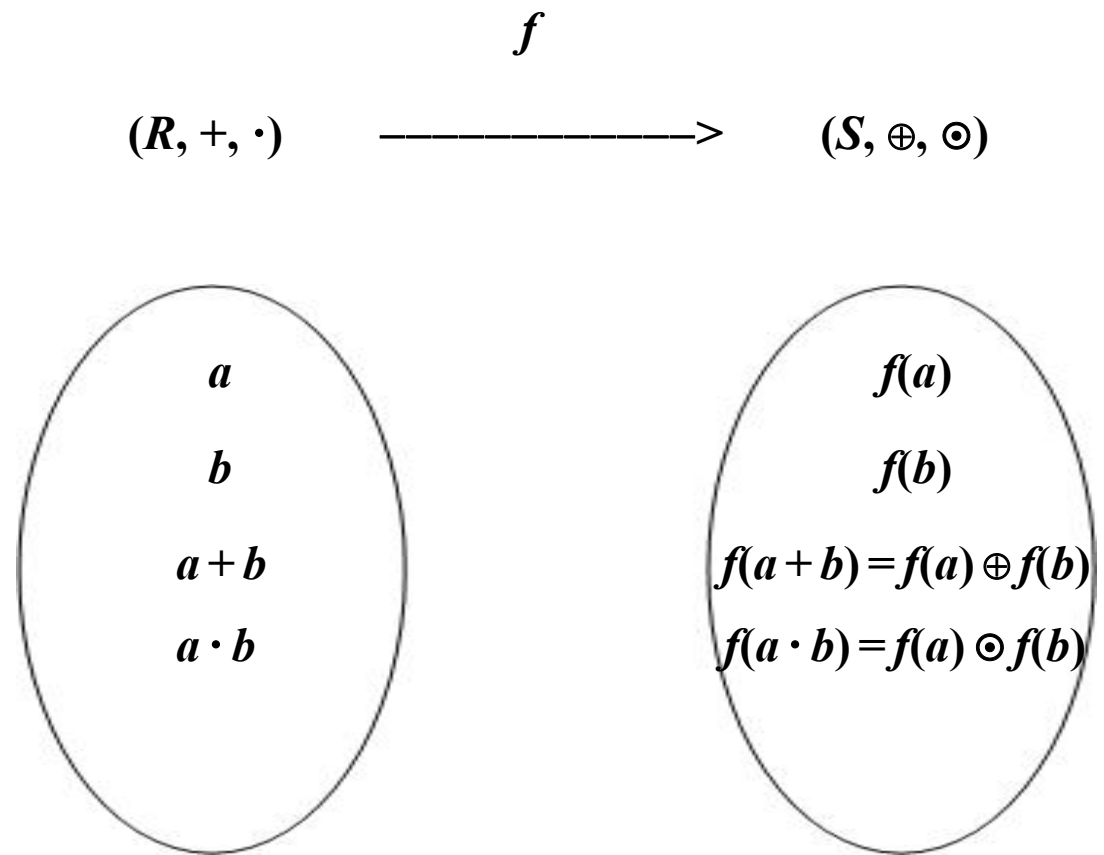
Suppose that $(R, +, \cdot)$ and (S, \oplus, \odot) are two rings.

A function $f: R \rightarrow S$ is a *ring homomorphism*,

if for all $a, b \in R$,

$$(a) \quad f(a + b) = f(a) \oplus f(b);$$

$$(b) \quad f(a \cdot b) = f(a) \odot f(b).$$



Performing $a + b$ ($a \cdot b$) in R and then mapping $a + b$ ($a \cdot b$) to S under f is “equivalent” to mapping a, b to S under f and then performing $f(a) + f(b)$ ($f(a) \cdot f(b)$) in S .

Ex. Consider $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Z}_6, +, \cdot)$.

Define $f: \mathbb{Z} \rightarrow \mathbb{Z}_6$ by $f(x) = [x]$.

For any $x, y \in \mathbb{Z}$,

$$f(x + y) = [x + y] = [x] + [y] = f(x) + f(y);$$

$$f(x \cdot y) = [x \cdot y] = [x] \cdot [y] = f(x) \cdot f(y).$$

So, f is a ring homomorphism.

Let $f: (R, +, \cdot) \rightarrow (S, \oplus, \odot)$ be a ring homomorphism.

If f is one-to-one and onto, then f is a ring isomorphism and R, S are said to be two isomorphic rings.

Ex. Consider the following ring $(R, +, \cdot)$.

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

\cdot	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Define $f: R \rightarrow Z_5$ as follows:

$$f(a) = [0], f(b) = [1], f(c) = [2], f(d) = [3],$$

$$\text{and } f(e) = [4].$$

Then, f is an isomorphism from R to Z_5 .

$$\text{For example, } f(c + d) = f(a) = [0] = [2] + [3] = f(c) + f(d)$$

$$\text{and } f(c \cdot d) = f(b) = [1] = [2] \cdot [3] = f(c) \cdot f(d).$$

For $(R, +, \cdot)$ and $a \in R$, we define

1. $0a = z$, $1a = a$, $(n+1)a = na + a$, and $(-n)a = n(-a)$,
where $n \geq 1$;
2. $a^0 = u$, $a^1 = a$, and $a^{n+1} = a^n \cdot a$.

Theorem. *If $f: (R, +, \cdot) \rightarrow (S, \oplus, \odot)$ is a ring homomorphism, then*

- (a) $f(z_R) = z_S$, where z_R and z_S are the zeros of R and S ;
- (b) $f(-a) = -f(a)$ for any $a \in R$;
- (c) $f(na) = nf(a)$ for any $a \in R$ and $n \in \mathbb{Z}$;
- (d) $f(a^n) = [f(a)]^n$ for any $a \in R$ and $n \in \mathbb{Z}^+$;
- (e) if A is a subring of R , $f(A)$ is a subring of S .

線代學過

Proof. (a) $z_S \oplus f(z_R) = f(z_R) = f(z_R + z_R) = f(z_R) \oplus f(z_R)$

$$\Rightarrow z_S = f(z_R).$$

(b) $f(a) \oplus f(-a) = f(a + (-a)) = f(z_R) = z_S$

$\Rightarrow f(-a)$ is the additive inverse of $f(a)$

$$\Rightarrow f(-a) = -f(a).$$

(c) By induction on $n (\geq 0)$,

$$n = 0, \quad f(0a) = f(z_R) = z_S = 0f(a);$$

$$n = k, \quad f(ka) = kf(a);$$

$$\begin{aligned} n = k + 1, \quad f((k + 1)a) &= f(ka + a) = f(ka) \oplus f(a) \\ &= kf(a) \oplus f(a) = (k + 1)f(a). \end{aligned}$$

$$\begin{aligned} \text{When } n > 0, \quad f((-n)a) &= f(n(-a)) = nf(-a) \\ &= n(-f(a)) = (-n)f(a). \end{aligned}$$

(d) Left as an exercise (also by induction on n).

(e) For any $x, y \in f(A)$, suppose $x = f(a)$ and $y = f(b)$,
where $a, b \in A$. Then,

$$x \oplus y = f(a) \oplus f(b) = f(a + b) \in f(A) \quad (\text{since } a + b \in A)$$

$$x \odot y = f(a) \odot f(b) = f(a \cdot b) \in f(A) \quad (\text{since } a \cdot b \in A)$$

$$-x = -f(a) = f(-a) \in f(A) \quad (\text{since } -a \in A)$$

$\Rightarrow f(A)$ is a subring of S .

Theorem. *If $f: (R, +, \cdot) \rightarrow (S, \oplus, \odot)$ is a ring homomorphism and onto, where $|S| > 1$, then*

- (a) *if R has unity u_R , $f(u_R)$ is the unity of S ;*
- (b) *if R has unity u_R and $a^{-1} \in R$ ($a \in R$), then*
$$f(a^{-1}) = [f(a)]^{-1} \in S;$$
- (c) *if R is commutative, then S is commutative;*
- (d) *if I is an ideal of R , then $f(I)$ is an ideal of S .*

Proof.

- (a) For any $s \in S$, there exists $r \in R$ with $f(r) = s$
(because f is onto).**

$$s \odot f(u_R) = f(r) \odot f(u_R) = f(r \cdot u_R) = f(r) = s.$$

Similarly, $f(u_R) \odot s = s$.

$\Rightarrow f(u_R)$ is the unity of S .

- (b) Suppose $b = a^{-1}$.**

$$\Rightarrow a \cdot b = b \cdot a = u_R$$

$$f(a) \odot f(b) = f(a \cdot b) = f(u_R) = u_S \quad (u_S \text{ is the unity of } S)$$

Similarly, $f(b) \odot f(a) = u_S$.

$$\Rightarrow (f(a^{-1}) =) f(b) = [f(a)]^{-1}$$

(c) left as an exercise.

(d) I is a subring of $R \Rightarrow f(I)$ is a subring of S .

Let $x \in f(I)$ and $y \in S$.

$\Rightarrow x = f(a)$ and $y = f(b)$, where $a \in I$ and $b \in R$
(because f is onto)

$$\begin{aligned}\Rightarrow x \odot y &= f(a) \odot f(b) \\ &= f(a \cdot b) \in f(I) \quad (\text{because } a \cdot b \in I).\end{aligned}$$

Similarly, $y \odot x \in f(I)$.

$\Rightarrow f(I)$ is an ideal of S .

Ex. Let C be the set of complex numbers and S be the set of real matrices of the form

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

$(C, +, \cdot)$ is a field and $(S, +, \cdot)$ is a ring.

Define $f: C \rightarrow S$ by $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

$$1. \quad f((a + bi) + (x + yi)) = f((a + x) + (b + y)i)$$

$$= \begin{bmatrix} a + x & b + y \\ -(b + y) & a + x \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

$$= f(a + bi) + f(x + yi).$$

$$2. \quad f((a + bi) \cdot (x + yi)) = f((ax - by) + (bx + ay)i)$$

$$= \begin{bmatrix} ax - by & bx + ay \\ -(bx + ay) & ax - by \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

$$= f(a + bi) \cdot f(x + yi).$$

3. f is one-to-one and onto.

$\Rightarrow f$ is a ring isomorphism.

We can compute $(4 + 5i)(2 - 3i)$ through matrix operations as follows.

$$\begin{aligned}(4 + 5i) \cdot (2 - 3i) &= f^{-1}f((4 + 5i) \cdot (2 - 3i)) \\&= f^{-1}(f(4 + 5i) \cdot f(2 - 3i)) \\&= f^{-1}\left(\begin{bmatrix} 4 & 5 \\ -5 & 4 \end{bmatrix} \begin{bmatrix} 2 & -3 \\ 3 & 2 \end{bmatrix}\right) \\&= f^{-1}\left(\begin{bmatrix} 23 & -2 \\ 2 & 23 \end{bmatrix}\right) \\&= 23 - 2i.\end{aligned}$$

Ex. (following the discussion of the Chinese remainder theorem)

$(Z_{32736}, +, \cdot)$ is a ring, where $32736 = 31 \times 32 \times 33$.

$(Z_{31} \times Z_{32} \times Z_{33}, \oplus, \odot)$ is a ring, where

$$([x_1], [x_2], [x_3]) \oplus ([y_1], [y_2], [y_3])$$

$$= ([x_1 + y_1] \text{ in } Z_{31}, [x_2 + y_2] \text{ in } Z_{32}, [x_3 + y_3] \text{ in } Z_{33});$$

$$([x_1], [x_2], [x_3]) \odot ([y_1], [y_2], [y_3])$$

$$= ([x_1 \cdot y_1] \text{ in } Z_{31}, [x_2 \cdot y_2] \text{ in } Z_{32}, [x_3 \cdot y_3] \text{ in } Z_{33}).$$

Define $f: (Z_{32736}, +, \cdot) \rightarrow (Z_{31} \times Z_{32} \times Z_{33}, \oplus, \odot)$ as follows:

$$f([x]) = ([x_1], [x_2], [x_3]), \text{ where } x_1 \equiv x \pmod{31};$$

$$x_2 \equiv x \pmod{32};$$

$$x_3 \equiv x \pmod{33}.$$

f is an isomorphism from Z_{32736} to $Z_{31} \times Z_{32} \times Z_{33}$.

(refer to Example 14.21 in page 700 of Grimaldi's book)

$[18152] \cdot [18153]$ in Z_{32736} can be computed as follows.

$$\begin{aligned}
& [18152] \cdot [18153] \\
&= f^{-1}f([18152] \cdot [18153]) \\
&= f^{-1}(f([18152]) \odot f([18153])) \\
&= f^{-1}([17], [8], [2]) \odot ([18], [9], [3]) \\
&= f^{-1}([17] \times [18] \text{ in } Z_{31}, [8] \times [9] \text{ in } Z_{32}, \\
&\quad [2] \times [3] \text{ in } Z_{33}) \\
&= f^{-1}([27], [8], [6]) \\
&= [25416]
\end{aligned}$$

(refer to the example of the Chinese remainder theorem)

In general, if $n = n_1 \times n_2 \times \dots \times n_k$, where $n_i > 1$ is an integer and $\gcd(n_i, n_j) = 1$, then $(\mathbb{Z}_n, +, \cdot)$ and $(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}, \oplus, \odot)$ are isomorphic.

As a result, computation on large integers in \mathbb{Z}_n can be achieved with (parallel) computation on smaller integers in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$.

(do Exercise #7)

Groups

• Definition

G : a nonempty set

\cdot : a binary operation

(G, \cdot) is called a *group* if the following hold.

1. Closure

For $a, b \in G$, $a \cdot b \in G$.

2. Associativity

For $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. Identity

There exists $e \in G$ with $a \cdot e = e \cdot a = a$ for all $a \in G$.

4. Inverse

For each $a \in G$, there exists $b \in G$ with $a \cdot b =$
 $b \cdot a = e$.

Let (G, \cdot) be a group.

If $a \cdot b = b \cdot a$ for all $a, b \in G$, then G is called a *commutative*, or *abelian*, group.

Ex. Under ordinary addition, each of Z, Q, R, C is an abelian group. None of them are groups under multiplication, because 0 has no multiplicative inverse.

Ex. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group
 $((R, \cdot)$ is a semigroup).

Ex. $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ is a set of six permutations on $\{1, 2, 3\}$, where

$$\begin{aligned} \pi_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \pi_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \pi_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ r_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & r_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & r_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

(G, \cdot) is a nonabelian group.

$$\pi_1 \cdot r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_3.$$

$$r_1 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = r_2.$$

\cdot	π_0	π_1	π_2	r_1	r_2	r_3
π_0	π_0	π_1	π_2	r_1	r_2	r_3
π_1	π_1	π_2	π_0	r_3	r_1	r_2
π_2	π_2	π_0	π_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	π_0	π_1	π_2
r_2	r_2	r_3	r_1	π_2	π_0	π_1
r_3	r_3	r_1	r_2	π_1	π_2	π_0

Ex. For each $n \in \mathbb{Z}^+$ and $n > 1$, $(\mathbb{Z}_n, +)$ is an abelian group. For each prime number $p > 1$, $(\mathbb{Z}_p - [0], \cdot)$ is an abelian group.

$n = 6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$p = 7$

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ex. Let $U_9 = \{[a] \mid [a] \in \mathbb{Z}_9 \text{ and } [a]^{-1} \text{ exists, i.e., } [a] \text{ is a unit in } \mathbb{Z}_9\} = \{[1], [2], [4], [5], [7], [8]\} = \{[a] \mid [a] \in \mathbb{Z}_9 \text{ and } \gcd(a, 9) = 1\}.$

Then, (U_9, \cdot) is an abelian group.

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Theorem. *For any group G ,*

- (a) the identity of G is unique;***
- (b) the inverse of each element of G is unique;***
- (c) if $a, b, c \in G$ and $a \cdot b = a \cdot c$, then $b = c$;***
- (d) if $a, b, c \in G$ and $b \cdot a = c \cdot a$, then $b = c$;***
- (e) G is abelian iff $(ab)^2 = a^2 \cdot b^2$ for all $a, b \in G$.***

Proof. Left as an exercise.

Let G be a group and H be a nonempty subset of G .

If H is a group under the binary operation of G , then H is a *subgroup* of G .

$\{e\}$ is said to be the *trivial subgroup* of G .

Ex. $G = (\mathbb{Z}_6, +)$ is an abelian group.

Let $H = \{[0], [2], [4]\}$, which is a subset of \mathbb{Z}_6 .

+	[0]	[2]	[4]
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

$(H, +)$ is a subgroup of G .

We use a^{-1} to denote the inverse of a .

Define $a^0 = e$, $a^1 = a$, $a^{n+1} = a^n \cdot a$ for $n \geq 1$, and $a^{-n} = (a^{-1})^n$.

Theorem. *If H is a nonempty subset of a group G , then H is a subgroup of G iff*

- (a) $a \cdot b \in H$ for all $a, b \in H$;
- (b) $a^{-1} \in H$ for all $a \in H$.

Proof. (if) closure : from (a)

associativity : from G

identity : $a \cdot a^{-1} = e \in H$

inverse : from (b)

(only if) trivial

Theorem. *Suppose that G is a group and H is a nonempty subset of G . If H is finite, then H is a subgroup of G iff H is closed under the binary operation of G .*

Proof. (if) Suppose $a \in H = \{h_1, h_2, \dots, h_n\}$,
where $n = |H|$ is finite.

$$a \cdot H = \{a \cdot h_1, a \cdot h_2, \dots, a \cdot h_n\} = H$$

$$\Rightarrow a \cdot h_i = a = a \cdot e \text{ for some } i$$

$$\Rightarrow h_i = e$$

$$\Rightarrow a \cdot h_j = e \text{ for some } j.$$

$$(h_j \cdot a)^2 = (h_j \cdot (a \cdot h_j)) \cdot a = (h_j \cdot e) \cdot a = h_j \cdot a$$

$$\Rightarrow h_j \cdot a = e = a \cdot h_j$$

$$\Rightarrow a^{-1} = h_j \in H$$

$$\Rightarrow H \text{ is a subgroup of } G.$$

(only if) trivial

Theorem. Let (G, \circ) and $(H, *)$ be two groups. Define the binary operation \cdot on $G \times H$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

Then, $(G \times H, \cdot)$ is a group.

Proof. Left as an exercise.

Ex. Consider the groups $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_3, +)$. Define \cdot on $\mathbb{Z}_2 \times \mathbb{Z}_3$ by $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. Then, $(\mathbb{Z}_2 \times \mathbb{Z}_3, \cdot)$ is a group with identity $([0], [0])$. The inverse, for example, of $([1], [2])$ is $([1], [1])$.

• Group Homomorphism

Suppose that (G, \circ) and $(H, *)$ are two groups.

$f: G \rightarrow H$ is a *group homomorphism*, if for all $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

Ex. Let $G = (Z, +)$ and $H = (Z_4, +)$.

Define $f: G \rightarrow H$ by $f(x) = [x]$.

For any $x, y \in G$,

$$f(x + y) = [x + y] = [x] + [y] = f(x) + f(y)$$

$\Rightarrow f$ is a group homomorphism.

Theorem. *Let (G, \circ) and $(H, *)$ be two groups with identities e_G and e_H , respectively. If $f: G \rightarrow H$ is a homomorphism, then*

- (a) $f(e_G) = e_H$;
- (b) $f(a^{-1}) = [f(a)]^{-1}$ for any $a \in G$;
- (c) $f(a^n) = [f(a)]^n$ for any $a \in G$ and $n \in \mathbb{Z}$;
- (d) $f(S)$ is a subgroup of H for any subgroup S of G .

Proof.

$$\begin{aligned} \text{(a)} \quad e_H * f(e_G) &= f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G) \\ &\Rightarrow e_H = f(e_G). \end{aligned}$$

(b), (c) Left as an exercise.

(d) Suppose $x = f(a), y = f(b) \in f(S)$, where $a, b \in S$.

$$x * y = f(a) * f(b) = f(a \circ b) \in f(S) \quad (a \circ b \in S)$$

$$x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S) \quad (a^{-1} \in S)$$

$$\Rightarrow f(S) \text{ is a subgroup of } H.$$

Suppose that $f: (G, \circ) \rightarrow (H, *)$ is a group homomorphism. If f is one-to-one and onto, then f is a *group isomorphism* and G, H are two *isomorphic groups*.

Ex. Define $f: (R^+, \cdot) \rightarrow (R, +)$ by $f(x) = \log_{10} x$.

- For $a, b \in R^+$, $f(a \cdot b) = \log_{10}(a \cdot b) = \log_{10} a + \log_{10} b = f(a) + f(b)$.

- f is one-to-one and onto

$\Rightarrow f$ is an isomorphism.

Ex. $G = (\{1, -1, i, -i\}, \cdot)$ is a group.

$H = (Z_4, +)$ is a group.

Define $f: G \rightarrow H$ by $f(1) = [0]$, $f(-1) = [2]$,

$f(i) = [1]$ and $f(-i) = [3]$.

$\Rightarrow f$ is an isomorphism.

For example, $f(i \cdot (-i)) = f(1) = [0] = [1] + [3] =$

$f(i) + f(-i)$.

Further, $(\{1, -1\}, \cdot)$ is a subgroup of G , and

$(f(\{1, -1\}), \cdot) = (\{[0], [2]\}, +)$ is a subgroup of H .

Notice that $i^1 = i$, $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$,

i.e., every element of G is a power of i .

It is said that i generates G and denoted by $G = \langle i \rangle$.

• Cyclic Groups

A group G is **cyclic**, if there is $a \in G$ such that for all $x \in G$, $x = a^k$ for some $k \in \mathbb{Z}$.

In this case, G is denoted by $G = \langle a \rangle (= \{a^i \mid i \in \mathbb{Z}\})$, and a is said to be **a generator of G .**

Ex. Consider the group $(\mathbb{Z}, +)$.

$$\mathbb{Z} = \langle 1 \rangle \quad \text{and} \quad \mathbb{Z} = \langle -1 \rangle.$$

For example, $3 = (1)^3 = 1 + 1 + 1.$

$$\begin{aligned} -3 &= (1)^{-3} = (-1)^3 \quad (a^{-n} = (a^{-1})^n) \\ &= (-1) + (-1) + (-1). \end{aligned}$$

$$\begin{aligned} 3 &= (-1)^{-3} = (-(-1))^3 = (1)^3 \\ &= 1 + 1 + 1. \end{aligned}$$

$$-3 = (-1)^3 = (-1) + (-1) + (-1).$$

Ex. Recall that $U_9 = \{[a] \mid [a] \in Z_9 \text{ and } [a]^{-1} \text{ exists}\} = \{[1], [2], [4], [5], [7], [8]\}$.

\cdot	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$$4 \cdot 5 = 2$$

$$\langle [1] \rangle = \{[1]\};$$

$$\langle [2] \rangle = \langle [5] \rangle = \{[1], [2], [4], [5], [7], [8]\} = U_9;$$

$$\langle [4] \rangle = \langle [7] \rangle = \{[1], [4], [7]\};$$

$$\langle [8] \rangle = \{[1], [8]\}.$$

$\Rightarrow (U_9, \cdot)$ is a cyclic group with two generators
[2] and [5].

Ex. Consider $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ again, where

$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

\cdot	π_0	π_1	π_2	r_1	r_2	r_3
π_0	π_0	π_1	π_2	r_1	r_2	r_3
π_1	π_1	π_2	π_0	r_3	r_1	r_2
π_2	π_2	π_0	π_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	π_0	π_1	π_2
r_2	r_2	r_3	r_1	π_2	π_0	π_1
r_3	r_3	r_1	r_2	π_1	π_2	π_0

$$\langle \pi_0 \rangle = \{\pi_0\}, \quad \langle \pi_1 \rangle = \langle \pi_2 \rangle = \{\pi_0, \pi_1, \pi_2\}$$

$$\langle r_1 \rangle = \{\pi_0, r_1\}, \quad \langle r_2 \rangle = \{\pi_0, r_2\}, \quad \langle r_3 \rangle = \{\pi_0, r_3\}$$

$\Rightarrow G$ is not cyclic

Suppose that (G, \cdot) is a cyclic group.

Then, G is abelian.

For example, if $G = \langle a \rangle$ and $x = a^u, y = a^v \in G$, then

$$x \cdot y = a^u \cdot a^v = a^{u+v} = a^{v+u} = a^v \cdot a^u = y \cdot x.$$

However, the converse is not always true.

For example, the following abelian group is not cyclic.

\cdot	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Theorem. *Let G be a group, $a \in G$, and $S = \{a^k \mid k \in \mathbb{Z}\}$. Then, S is a subgroup of G . This subgroup is called the subgroup generated by a and denoted by $\langle a \rangle$.*

Proof. Let $x = a^m \in S$ and $y = a^n \in S$.

$$(1) \quad x \cdot y = a^m \cdot a^n = a^{m+n} \in S.$$

$$(2) \quad x^{-1} = a^{-m} \in S.$$

$\Rightarrow S$ is a subgroup.

If G is a group and $a \in G$, the *order* of a , denoted by $o(a)$, is $|\langle a \rangle|$. If $|\langle a \rangle|$ is infinite, we say that a has infinite order.

Theorem. Let a be an element in a group G , and suppose $a^n = e$ for some positive integer n . If m is the least positive integer such that $a^m = e$, then

- (a) $\langle a \rangle$ has order m and $\langle a \rangle = \{a^0 = e = a^m, a^1, a^2, \dots, a^{m-1}\}$;
- (b) $a^s = a^t$ iff $s \equiv t \pmod{m}$. ($\Rightarrow m \mid n$)

Proof. (1) $a^0, a^1, a^2, \dots, a^{m-1}$ are all distinct.

If $a^i = a^j$ for some i, j , $0 \leq i < j \leq m-1$,

then $a^{j-i} = a^j \cdot a^{-i} = e$, a contradiction.

(2) For any integer k , $a^k = a^r$ for some $0 \leq r \leq m-1$,
where $k = mq + r$ (i.e., $k - r \equiv 0 \pmod{m}$) and q is
an integer.

$$a^k = a^{mq+r} = a^{mq} a^r = a^r.$$

$$(1), (2) \Rightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{m-1}\}$$

(i.e., $\langle a \rangle$ has order m) and

$$a^s = a^t \text{ iff } s - t \equiv 0 \pmod{m}$$

$$\text{iff } s \equiv t \pmod{m}.$$

Theorem. *Let G be a cyclic group.*

(a) *If G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$.*

(b) *If $|G| = n$, then G is isomorphic to $(\mathbb{Z}_n, +)$.*

Proof. (a) Let $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

(1) $a^i \neq a^j$ for all $i \neq j$.

if $a^i = a^j$ for $i \neq j$, then

$$a^{j-i} = a^j \cdot a^{-i} = e. \quad (\text{assume } j > i)$$

$\Rightarrow G$ is finite, a contradiction!

(2) Define $f: G \rightarrow \mathbb{Z}$ by $f(a^k) = k$.

$$f(a^m \cdot a^n) = f(a^{m+n}) = m + n = f(a^m) + f(a^n).$$

(3) f is one-to-one and onto

$\Rightarrow f$ is an isomorphism

(b) Left as an exercise.

Ex. Recall that $U_9 = \{[a] \mid [a] \in Z_9 \text{ and } [a]^{-1} \text{ exists}\} = \{[1], [2], [4], [5], [7], [8]\}$.

\cdot	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

There is an isomorphism f from (U_9, \cdot) to $(Z_6, +)$ as follows:

$$\begin{aligned} f([1]) &= f([2^0]) = [0]; & f([2]) &= f([2^1]) = [1]; \\ f([4]) &= f([2^2]) = [2]; & f([5]) &= f([2^5]) = [5]; \\ f([7]) &= f([2^4]) = [4]; & f([8]) &= f([2^3]) = [3]. \end{aligned}$$

For example, $f([2] \cdot [7]) = f([5]) = [5] = [1] + [4] = f([2]) + f([7]);$

$$f([4] \cdot [5]) = f([2]) = [1] = [2] + [5] = f([4]) + f([5]).$$

Theorem. *Any subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$ be a cyclic group and H be a subgroup of G .

If $H = \{e\}$, then H is cyclic.

So, we assume $H \neq \{e\}$,

To show that H is cyclic, we need to find a generator for H .

Let t be the smallest positive integer such that $a^t \in H$.

We show below that a^t is a generator for H .

$$(1) \quad \langle a^t \rangle \subseteq H$$

by the closure property

$$(2) \quad \langle a^t \rangle \supseteq H$$

If $a^s \in H$, where $s = qt + r$ ($q, r \in \mathbb{Z}$) and $0 < r < t$,

then $a^r = a^s \cdot a^{-qt} = a^s \cdot (a^{-t})^q \in H$, a contradiction

(i.e., $r = 0$).

$$(1), (2) \Rightarrow H = \langle a^t \rangle.$$

- **Cosets and Lagrange's Theorem**

Lagrange's Theorem :

*If H is a subgroup of a finite group G , then
 $|H|$ divides $|G|$.*

Suppose that H is a subgroup of G .

For any $a \in G$, the set $a \cdot H = \{a \cdot h \mid h \in H\}$

$(H \cdot a = \{h \cdot a \mid h \in H\})$ is a *left coset* (*right coset*) of H in G .

Ex. Suppose $G = (Z_{12}, +)$ and $H = \{[0], [4], [8]\}$ is a subgroup of G .

$$[0] + H = \{[0], [4], [8]\} = H.$$

$$[4] + H = \{[0], [4], [8]\} = H.$$

$$[8] + H = \{[0], [4], [8]\} = H.$$

$$[1] + H = [5] + H = [9] + H = \{[1], [5], [9]\}.$$

$$[2] + H = [6] + H = [10] + H = \{[2], [6], [10]\}.$$

$$[3] + H = [7] + H = [11] + H = \{[3], [7], [11]\}.$$

$$\{H, \{[1], [5], [9]\}, \{[2], [6], [10]\}, \{[3], [7], [11]\}\}$$

forms a partition of G .

Ex. Consider $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ again, where

$$\begin{aligned}\pi_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \pi_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \pi_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ r_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & r_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & r_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.\end{aligned}$$

$H = \{\pi_0, \pi_1, \pi_2\}$ is a subgroup of G .

$$\pi_0 H = \{\pi_0 \pi_0, \pi_0 \pi_1, \pi_0 \pi_2\} = \{\pi_0, \pi_1, \pi_2\} = H.$$

$$\pi_1 H = \pi_2 H = H.$$

$$r_1 H = r_2 H = r_3 H = \{r_1, r_2, r_3\}.$$

$\{H, \{r_1, r_2, r_3\}\}$ forms a partition of G .

$K = \{\pi_0, r_1\}$ is a subgroup of G .

$$Kr_2 = \{\pi_0 r_2, r_1 r_2\} = \{r_2, \pi_1\}.$$

$$r_2 K = \{r_2 \pi_0, r_2 r_1\} = \{r_2, \pi_2\}.$$

$$\Rightarrow Kr_2 \neq r_2 K.$$

Theorem. *If H is a subgroup of a finite group G , then for any $a, b \in G$,*

(a) $|aH| = |H|;$

(b) $|Ha| = |H|;$

(c) $aH = bH$ or $aH \cap bH = \emptyset;$

(d) $Ha = Hb$ or $Ha \cap Hb = \emptyset.$

Proof. (a) Let $h_i, h_j \in H$.

$$h_i \neq h_j \Rightarrow ah_i \neq ah_j. \quad \therefore |aH| = |H|.$$

(b) analogous to (a).

(c) Assume $aH \cap bH \neq \emptyset$.

Let $c = ah_1 = bh_2$, where $h_1, h_2 \in H$.

If $x = ah_3 \in aH$, where $h_3 \in H$, then

$$x = (bh_2h_1^{-1})h_3 = b(h_2h_1^{-1}h_3) \in bH,$$

i.e., $aH \subseteq bH$.

Similarly, $aH \supseteq bH$.

$$\Rightarrow aH = bH$$

(d) analogous to (c).

Theorem. *Let H be a subgroup of a finite group G .*

- (a)** *The distinct left cosets of H in G form a partition of G .*
- (b)** *The distinct right cosets of H in G form a partition of G .*

Proof. **(a)** **(i)** $e \in H$, where e is the identity of G .

(ii) For each $g \in G$, $g \in gH$.

(iii) $aH = bH$ or $aH \cap bH = \emptyset$,

where $a, b \in G$.

(i), (ii), (iii) \Rightarrow distinct left cosets of H in G
form a partition of G .

(b) analogous to **(a)**.

Theorem. (Lagrange's Theorem) *Let H be a subgroup of a finite group G . Then, $|H|$ divides $|G|$.*

Proof. (i) $|aH| = |H|$ for all $a \in G$.

(ii) Distinct left cosets of H in G form a partition of G .

(i), (ii) $\Rightarrow |H|$ divides $|G|$.

Corollary. *If G is finite and $a \in G$, then $o(a)$ divides $|G|$.*

Corollary. *Any group of prime order is cyclic.*

Lagrange's theorem is useful in finding all the subgroups of a finite group.

Ex. Consider $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ again, where

$$\begin{aligned} \pi_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \pi_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \pi_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ r_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & r_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & r_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

Find all of the subgroups of G .

$|G| = 6 \Rightarrow$ any subgroup of G has 1, 2, 3 or 6 elements.

2, 3 are prime \Rightarrow the subgroups of G that have 2 or 3 elements are cyclic.

of elements = 1 : $\{\pi_0\}$.

of elements = 6 : G .

of elements = 2 or 3 : $\langle \pi_1 \rangle = \langle \pi_2 \rangle = \{\pi_0, \pi_1, \pi_2\}$.

$$\langle r_1 \rangle = \{\pi_0, r_1\}.$$

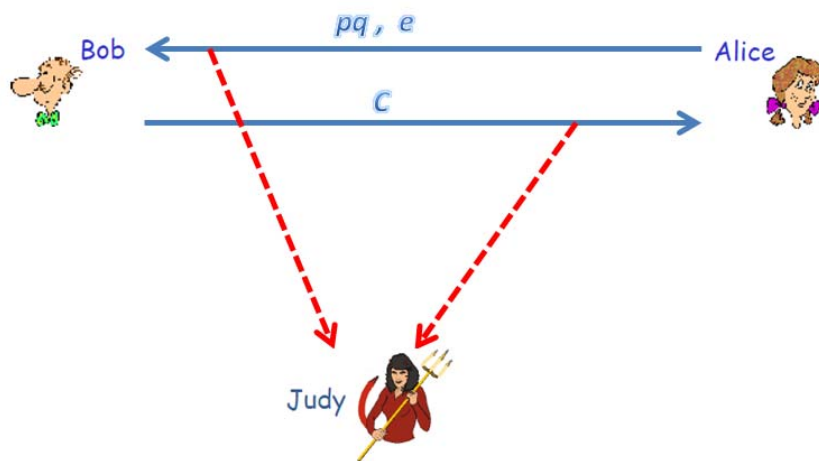
$$\langle r_2 \rangle = \{\pi_0, r_2\}.$$

$$\langle r_3 \rangle = \{\pi_0, r_3\}.$$

• RSA Cryptosystem

Bob wants to send a message L to Alice, but Judy is the intruder.

(e.g., $L = 12$)



Step 1: Alice arbitrarily generates two prime integers p, q and calculates $\phi(pq)$, where ϕ is the Euler's phi function.
(e.g., $p = 5, q = 7$, and $\phi(pq) = 24$)

Step 2: Alice arbitrarily generates a pair of e (encryption key), d (decryption key), satisfying the following constraints.

- e is relatively prime to $\phi(pq)$.

(e.g., $e = 5$)

- $ed \equiv 1 \pmod{\phi(pq)}$

(e.g., $d = 29$)

Step 3: Alice broadcasts pq, e .

Step 4: Bob computes and broadcasts C (ciphertext),

where $C \equiv L^e \pmod{pq}$ and $0 \leq C < pq$.

(e.g., $C = 17$)

Step 5: Alice computes L (plaintext) from C as follows:

$$L \equiv C^d \pmod{pq},$$

where $0 \leq L < pq$.

Although Judy overhears e, pq, C , she is not able to obtain plaintext L without knowing d , even if she is aware of the two relations: $ed \equiv 1 \pmod{\phi(pq)}$ and $L \equiv C^d \pmod{pq}$.

If Judy wants to compute d , she must have $\phi(pq)$ available whose value can be calculated as

$$pq \times \left(1 - \frac{1}{p}\right) \times \left(1 - \frac{1}{q}\right),$$

which relies on p, q . However, it is very time-consuming to obtain p and q from pq .

(do Exercise #8)