Group

Chapter 16.1-3

부산대학교
PUSAN NATIONAL UNIVERSITY

Group

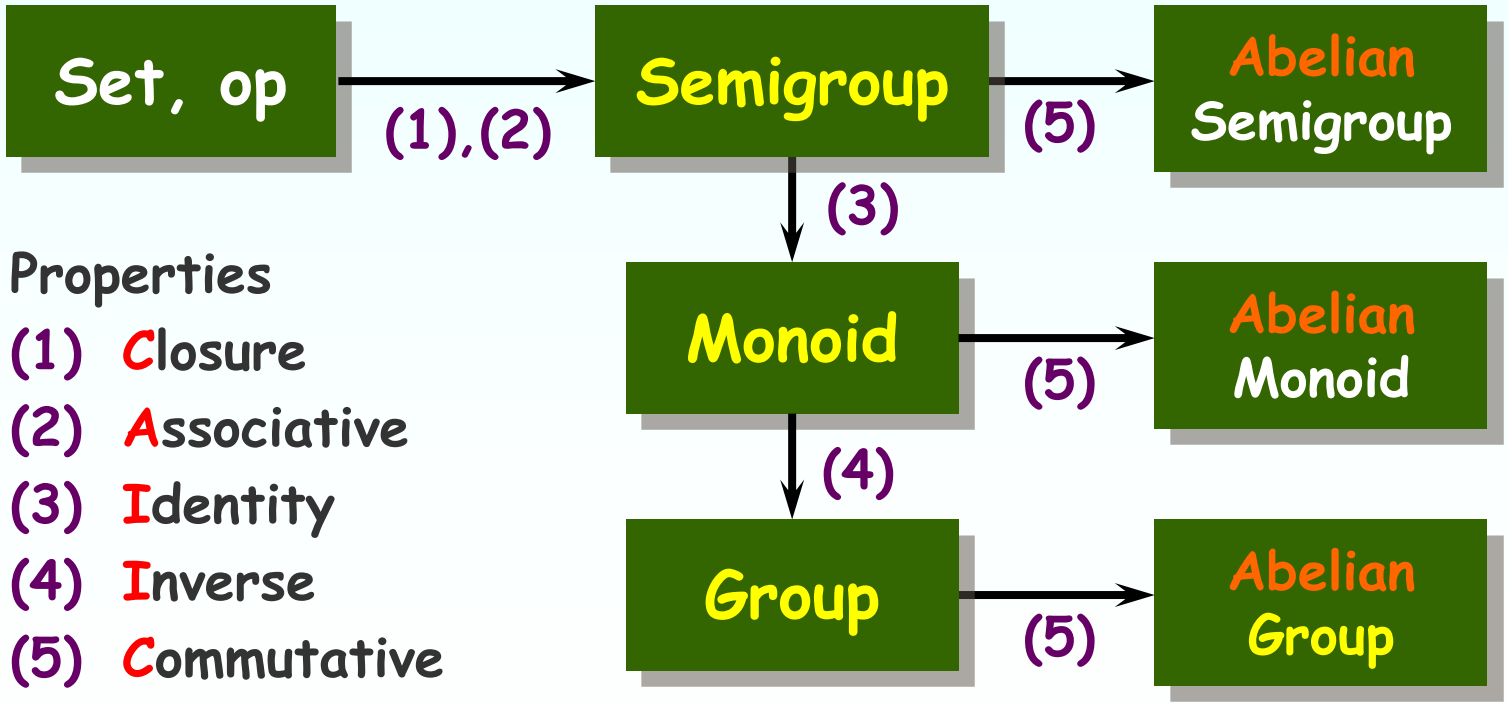
- **Definition 16.1**

  If G is a nonempty set and $\square$ is a binary operation on G, then $\langle G,\square \rangle$ is called a *group* if the following conditions are satisfied.

  1. For all $a,b \in G$, $a \square b \in G$ (Closure under $\square$)
  2. For all $a, b, c \in G$, $(a \square b) \square c = a \square (b \square c)$. (Associative)
  3. There exists $e \in G$ with $e \square a = a \square e = a$ for all $a \in G$. (Existence of an Identity)
  4. For each $a \in G$, there is an elements $a' \in G$ such that $a' \square a = a \square a' = e$. (Existence of Inverses)

Abelian Group

- Abelian Group
  - 5. A group <G,▫> is abelian if ▫ is Commutative.
    i.e., $a \square b = b \square a$ for all $a, b \in G$.



Properties
(1) Closure
(2) Associative
(3) Identity
(4) Inverse
(5) Commutative

$<Z_n, +>$

- For $n \in Z^+$, $n > 1$, we find that

  $<Z_n, +>$ is an abelian group.

  Associative

  Identity : 0

  Inverse exists in Z_n.

  - $(-a)$ for all a in Z_n
  - We can also subtract element in Z_n.
  - We define $a-b$ in Z_n to be $(a + (-b)) \bmod n$.

  Commutative

$<Z_n^*, \cdot>$

- **Theorem :**

  If n is any positive integer,

  $<Z_n^*, \cdot>$ is an abelian group.

- **Example : The multiplication table of Z_9^* is**

	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

$< Z_9^*, \cdot >$

1) Closed
2) Associative
3) Identity
4) Inverse
5) Commutative

Order of Group

- **Definition 16.2**

  For every group G the number of elements in G is called the *order of* G and is denoted by $|G|$.

  When the number of elements in a group is not finite we say that G has infinite order.

  (Example 16.3)

  For all $n \in Z^+$, $|\langle Z_n, + \rangle| = n$.

  $|\langle Z_p^*, \cdot \rangle| = p-1$.

- Notice that $|\langle Z_n^*, \cdot \rangle| = \phi(n)$.

Properties of Groups

- For every group G,
  - (1) The identity of G is unique
  - (2) The inverse of each element of G is unique
  - (3) If $ab = ac$ for $a,b,c \in G$ ➔ $b = c$
    (Left-cancellation property)
  - (4) If $ba = ca$ for $a,b,c \in G$ ➔ $b = c$
    (Right-cancellation property)

  (Notation) $a \square b \rightarrow ab$

  $a \square b = a \square c \rightarrow b = c$

Properties of Groups

(Proof)

(1) If e and e' are both identities in G,

then $e = ee' = e'$

(2) Let $a \in G$ and suppose that b, c are both inverses of a,

then $b = be = b(ac) = (ba)c = ec = c$

(Note)

The properties (3),(4) imply that each group element appears exactly once in each row and each column of the table for a finite group

Properties of Groups

- Example : $< Z_9^*, \cdot >$

$ab = ac \rightarrow b = c$, $ba = ca \rightarrow b = c$

	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

$ab = ac$

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$

$eb = ec$

$b = c$

$b \neq c \rightarrow ab \neq ac$

Properties of Groups

- Example : $<\{T,F\}, \wedge>$ abelian monoid, not a group

$\wedge$	F	T
F	F	F
T	F	T

1) Closed
2) Associative
3) Identity
4) Inverse
5) Commutative

$$F \wedge F = F \wedge T$$

$$F \wedge F = T \wedge F$$

Subgroup

- **Definition 16.3**

  Let G be a group and a non-empty set $H \subseteq G$.

  If H is a group under the binary operation on G, then we call H a subgroup of G.

  (Examples)

  - Every group G has trivial subgroups: $\{e\}$ and G
  - The group $\langle Z, + \rangle$ is a subgroup of $\langle Q, + \rangle$ and $\langle Q, + \rangle$ is a subgroup of $\langle R, + \rangle$
  - $G = \langle Z_6, + \rangle$, $H = \{0, 2, 4\}$

Examples

$< \{e\}, \square >$

1) Closed

$$e \square e = e$$

2) Associative

3) Identity

4) Inverse

$G = <Z_6, +>$, $H = \{0,2,4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Subgroup Condition (I)

- **Theorem 16.2**

  If H is a nonempty subset of a group G, then

  H is a subgroup of G ⟷

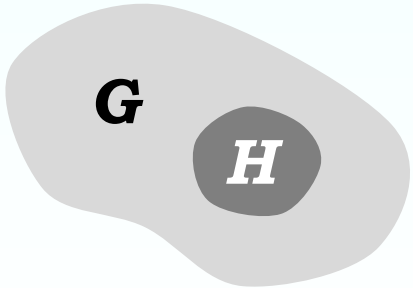
  (a) for all $a, b \in H$, $ab \in H$, (closed) and

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

  - Proof : See the text…

    inheritance of associative property

    $a\,a^{-1} = e \in H$; exist identity



Subgroup Condition (II)

- **Theorem 16.3**

  If H is a nonempty **finite** subset of a group G, then

  H is a subgroup of G ⟷

  H is **closed** under the binary operation on G.

(Ex.) $G = \langle Z_6, + \rangle$, $H = \{0,2,4\}$

+	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	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Subgroup Condition (II)

$G = \langle Z_6, + \rangle$, $H = \{0,2,4\}$

+	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

Unique **identity**

Unique **inverse**

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$= 2H = H$

distinct

$b \neq c$

$\Rightarrow ab \neq ac$

$5H = \{1,3,5\} = 1H$

$aH = \{ah \mid a \in G, h \in H\}$: a **coset** of H in G

$2H$?

Subgroup Condition (II)

(Proof of ←)

If $a \in H$, then $aH = \{ah \mid h \in H\} \subseteq H$ because of the closure condition. By the left-cancellation in G, if $h_1 \neq h_2$, then $ah_1 \neq ah_2$. So $|aH| = |H|$ and furthermore $aH = H$.

If $a \in H$, then there exists $b \in H$ with $ab = a$. But (in G) $ab = a = ae$, so $b = e$. Therefore there exist an identity element e in H.

There is an element $c \in H$ such that $ac = e$. Then $(ca)^2 = (ca)(ca) = c(ac)a = (ce)a = ca = (ca)e$, so $ca = e$. Thus a has its inverse (= c).

From the theorem 16.2, H is a subgroup of G.

Direct Product of Groups

- **Theorem 16.4**

  Let $\langle G, \square \rangle$ and $\langle H, * \rangle$ be groups.

  Define an operation $\blacklozenge$ on $G \times H$ by

  $$(g_1, h_1) \blacklozenge (g_2, h_2) = (g_1 \square g_2, h_1 * h_2)$$

  Then $\langle G \times H, \blacklozenge \rangle$ is a group and is called the direct product of G and H

  (Example)

  On $G = \langle Z_2, + \rangle \times \langle Z_9^*, \cdot \rangle$,

  - $(0,2) \blacklozenge (1,7) = (0+1,\ 2 \cdot 7) = (1,5)$
  - G is a group of order 12(=2x6)
  - Identity is (0,1) and Inverse of (1,2) is (1,5)

Direct Product of Groups

(Another Example)

On a direct product of four $\langle Z_2, + \rangle$'s

$G = \langle Z_2, + \rangle \times \langle Z_2, + \rangle \times \langle Z_2, + \rangle \times \langle Z_2, + \rangle \equiv \langle Z_2^4, + \rangle$,

- $(1,1,0,0) \equiv 1100 \in \langle Z_2^4, + \rangle$
- $1100 \blacklozenge 1010 = 0110$
- Error correction, Hamming distance, etc

$$\begin{array}{r} 1100 \\ 1010 \\ \hline 0110 \end{array}$$

+	0	1
0	0	1
1	1	0

Powers of Elements

- Definition of a^n

  For a group G, $a \in G$ and $n \in Z$,

  $a^0 = e$, $a^1 = a$, $a^2 = aa$, $a^{n+1} = a^n a$,

  $a^{-n} = (a^{-1})^n$, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$

  - Examples for $<Z_4, +>$

    $[3]^2=[3]+[3]=[6]=[2]$, $[3]^{-2}=[3^{-1}]^2=[1]^2=[2]$

    $[3]^2\,[3]^{-2}=[3]^{2-2}=[3]^0=$

- $(ab)^n = a^n b^n$?

  $([2]+[3])^2 = [2]^2 + [3]^2$?

  $(ab)^n = (ab)(ab)(ab)\cdots(ab) = aa\cdots abb\cdots b = a^n b^n$

  , if it is abelian

Homomorphism

- **Definition 16.4**

  If $\langle G, \square \rangle$ and $\langle H, * \rangle$ are groups and $f : G \to H$, then f is called a group homomorphism if for all $a, b \in G$, $f(a \square b) = f(a) * f(b)$.

  (Example)

  Consider $\langle Z, + \rangle$ and $\langle Z_4, + \rangle$. Define $f : Z \to Z_4$ by

  $$f(x) = [x] = \{ x+4k \mid k \in Z \}.$$

  For all $a,b \in Z$, $f(a+b) = [a+b] = [a]+[b] = f(a)+f(b)$.

  $$f(7+5) = [7+5] = [7]+[5] = f(7)+f(5)$$

Properties of Homomorphism

- **Theorem 16.5**

  Let $\langle G, \square \rangle$ and $\langle H, * \rangle$ be groups with respective identities e_G, e_H. If $f : G \to H$ is a homomorphism, then

  (1) $f(e_G) = e_H$ (2) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

  (3) $f(a^n) = [f(a)]^n$ for all $a \in G$ and all $n \in Z$

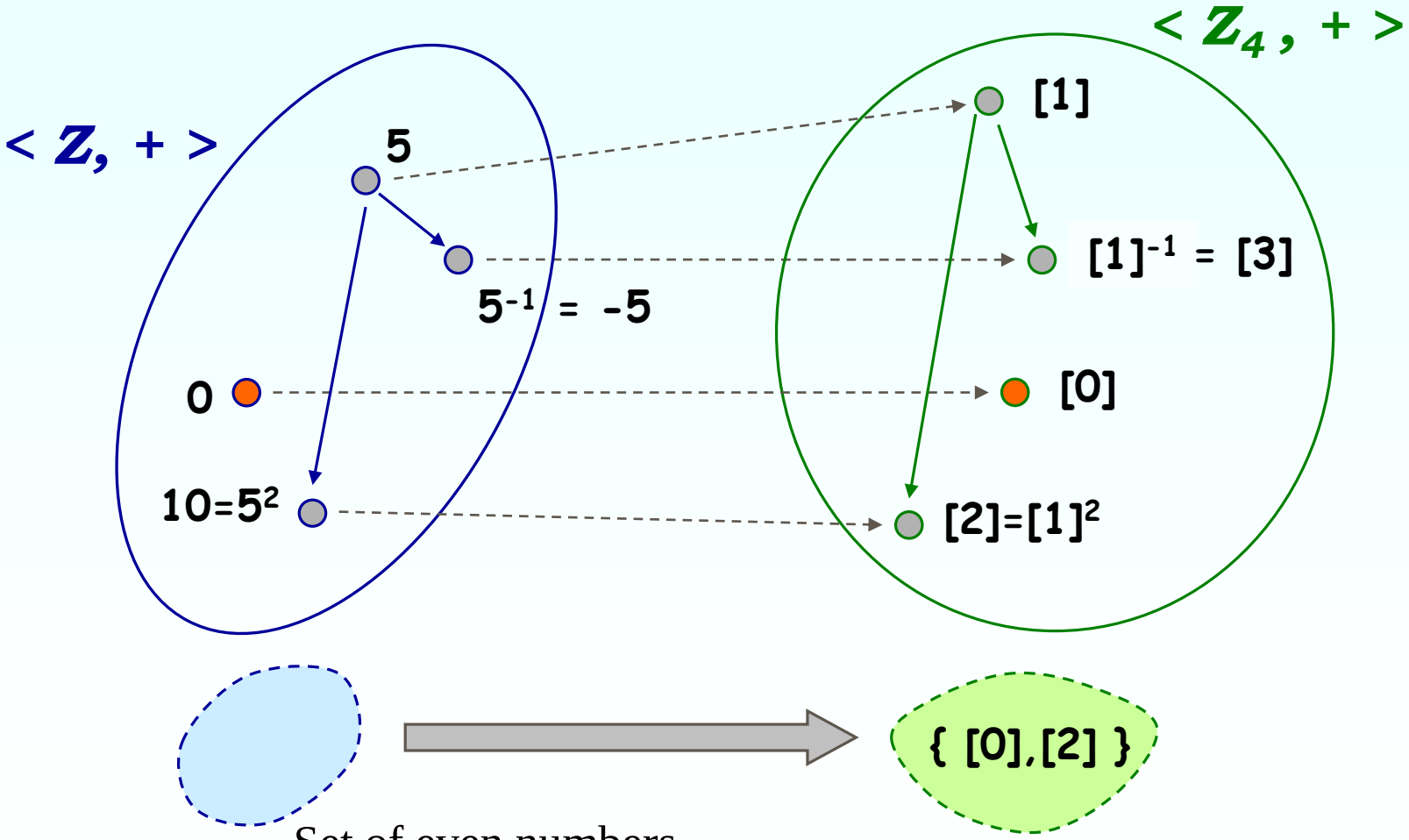
  (4) $f(S)$ is a subgroup of H for each subgroup S of G

  - For the example $f : Z \to Z_4$,

    $f(0)=[0]$,
    $f(5^{-1})=f(-5)=[-5]=[3]=[1]^{-1}=[5]^{-1}=[f(5)]^{-1}$,
    $f(5^3)=[5^3]=[5+5+5]=[5]+[5]+[5]=[5]^3=[f(5)]^3$

Properties of Homomorphism

An Example $f : Z \rightarrow Z_4$



Isomorphic Groups

- **Definition 16.5**

  If $f : \langle G, \square \rangle \rightarrow \langle H, * \rangle$ is a homomorphism, we call f an isomorphism if it is one-to-one and onto.

  In this case G, H are said to be isomorphic groups.

  (Example)

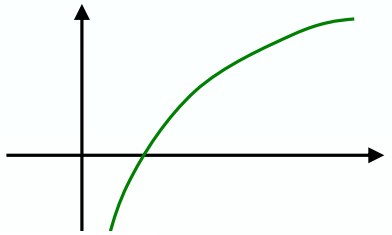
  Let $f : \langle R^+, \cdot \rangle \rightarrow \langle R, + \rangle$ where $f(x) = \log_{10}(x)$

  For all $a, b \in R^+$,

  $f(ab) = \log_{10}(ab) = \log_{10}(a) + \log_{10}(b) = f(a)+f(b)$

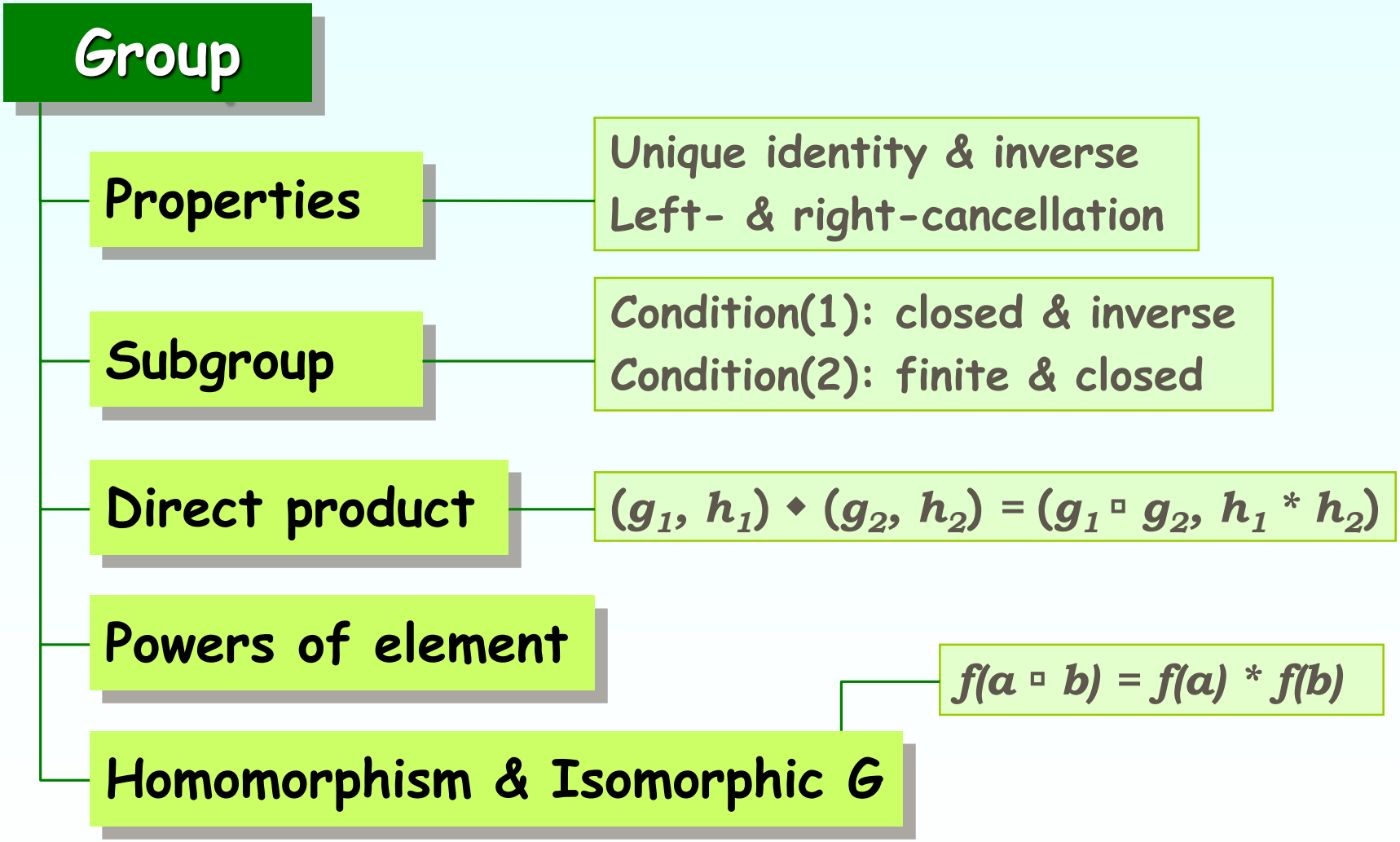
  This function is one-to-one and onto.

  Therefore, f is an isomorphism.



$f : A \rightarrow B$ is one-to-one iff for all $x, y \in A$, $f(x) = f(y) \Rightarrow x = y$

?


Group
Properties
Unique identity & inverse
Left- & right-cancellation
Subgroup
Condition(1): closed & inverse
Condition(2): finite & closed
Direct product
$(g_1, h_1) \blacklozenge (g_2, h_2) = (g_1 \square g_2, h_1 * h_2)$
Powers of element
$f(a \square b) = f(a) * f(b)$
Homomorphism & Isomorphic G

Cyclic Group

- **Definition 16.6**

  A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in Z$.

  Such an element x is called a generator (or primitive element) for G.

  A set $S = \{ a^k \mid k \in Z \}$ for $a \in G$ is a subgroup of G, because it is closed and satisfies the inverse property. (Refer to theorem 16.2) $a^k a^{-k} = a^0 = e$

  This subgroup is called the subgroup generated by a and is designated by $\langle a \rangle$.

Example

$3^{-2} = ?$

- Group $<Z_4, +>$ $\therefore$ Cyclic Group

$0^1 = 0 = e = 0^2 = 0^3 = 0^4$ ➔ $<0> = <\{0\}, +>$

$1^1 = 1,\ 1^2 = 1+1 = 2,$

$1^3 = 3,\ 1^4 = 4 = 0 = e$ ➔ $<1> = Z_4$

$2^1 = 2,\ 2^2 = 2+2 = 4 = 0 = e,$

$2^3 = 2^2 2^1 = 0+2 = 2,\ 2^4 = 8 = 0$ ➔ $<2> = \{0,2\}$

$3^1 = 3,\ 3^2 = 3+3 = 6 = 2,$

$3^3 = 9 = 1,\ 3^4 = 12 = 0 = e$ ➔ $<3> = Z_4$

Order of Elements

- **Definition 16.7**

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

- $\langle a \rangle = \{ a, a^2, \ldots, a^{ord(a)} (= e) \}$

  Let n be the smallest positive integer such that $a^n = e$.

  There are at most n elements in $\langle a \rangle$ since $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = a^r$ for $0 \le r < n$ and $k \in Z^+$.

  Meanwhile, for $0 \le i < j < n$, $a^j = a^i a^{(j-i)} \neq a^i$ because $a^{(j-i)} \neq e$ for $j - i < n$. Thus $ord(a) = n$ and $a^{ord(a)} = e$.

  Therefore, $\langle a \rangle = \{ a, a^2, \ldots, a^{ord(a)} (= e) \}$

Order of Elements

- **Theorem 16.6**

  Let $a \in G$ with $ord(a) = n$.

  If $m \in Z$ and $a^m = e$, then $n \mid m$.

  By the division algorithm, we have $m = qn + r$ for $0 \leq r < n$ and so it follows that $e = a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$.

  Thus $r = 0$ and $m = qn$. Therefore, $n \mid m$.

Example

- Group $\langle Z_4, + \rangle$

$1^1 = 1,\ 1^2 = 1+1 = 2,$

$1^3 = 3,\ 1^4 = 4 = 0 = e \rightarrow \langle 1 \rangle = Z_4$

$ord(1) = 4.$

$2^1 = 2,\ 2^2 = 2+2 = 4 = 0,$

$2^3 = 6 = 2,\ 2^4 = 8 = 0 = e \rightarrow \langle 2 \rangle = \{0,2\}$

$ord(2) = 2.$

$$a^{k\ ord(a)} = e$$

Theorems for Cyclic Groups

- **Theorem 16.7**

  Let G be a cyclic group.
  (a) If $|G|$ is infinite, then G is isomorphic to $\langle Z, + \rangle$.
  (b) If $|G| = n > 1$, then G is isomorphic to $\langle Z_n, + \rangle$.

(Proof (a)) An infinite cyclic group with a generator g can be represented as $G = \langle g \rangle = \{g^k \mid k \in Z\}$, where $g^m \neq g^n$ for $m \neq n$. Let $f : G \rightarrow Z$ be defined by $f(g^k) = k$. For $g^m, g^n \in G$, $f(g^m g^n) = f(g^{m+n}) = m+n = f(g^m) + f(g^n)$, so f is a homomorphism. f is one-to-one, because $g^m = g^n$ for $m = n$. For any $m \in Z$, there is $g^m \in G$ such that $f(g^m) = m$, so f is onto. Therefore, G is isomorphic to $\langle Z, + \rangle$.

Theorems for Cyclic Groups

- **Theorem 16.7**

  Let G be a cyclic group.
  (a) If $|G|$ is infinite, then G is isomorphic to $\langle Z, + \rangle$.
  (b) If $|G| = n > 1$, then G is isomorphic to $\langle Z_n, + \rangle$.

(Proof (b)) An finite cyclic group with a generator g can be represented as $G = \langle g \rangle = \{g^1, g^2, \ldots, g^n (= e)\}$. Let a function $f: G \rightarrow Z_n$ be defined by $f(g^k) = [k]$. For $g^m, g^n \in G$, $f(g^m g^n) = f(g^{m+n}) = [m+n] = [m] + [n] = f(g^m) + f(g^n)$, so f is a homomorphism. f is one-to-one, because $g^m = g^n$ for $[m] = [n]$. For any $[m]$ $(1 \leq m \leq n) \in Z_n$, there is $g^m \in G$ such that $f(g^m) = [m]$, so f is onto. Therefore, G is isomorphic to $\langle Z_n, + \rangle$.

Examples

(Ex.1) $G = \{ 2k \mid k \in Z \} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$<G, +>$ is an infinite cyclic group.

$G = \{ 2^k \mid k \in Z \}$

$f(2^k) = k \Rightarrow f : G \rightarrow Z$

$\{\ldots, -4, -2, 0, 2, 4, \ldots\} \rightarrow \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

(Ex.2) $Z_{10}^* = \{ 1, 3, 7, 9 \}$

$< Z_{10}^*, \cdot >$ is a finite cyclic group.

$Z_{10}^* = \{ 3^1, 3^2, 3^3, 3^4 \}$

$f(3^k) = [k] \Rightarrow f : Z_{10}^* \rightarrow Z_4$

$\{ 3^1, 3^2, 3^3, 3^4 \} \rightarrow \{0, 1, 2, 3\} = Z_4$

Theorems for Cyclic Groups

- **Theorem 16.8**

  Every subgroup of cyclic group is cyclic.

(Proof)

Let $G = \langle g \rangle$ with a generator g. If H is a subgroup of G, each element of H has the form g^k, for some $k \in Z$. For $H \neq \{e\}$, let t be the smallest positive integer such that $g^t \in H$. Then $\langle g^t \rangle \subseteq H$.

Let $b (= g^s) \in H$, for some $s \in Z$. By the division algorithm, $s = qt + r$, where $q, r \in Z$ and $0 \leq r < t$. So $g^r = g^{-qt} g^s = (g^t)^{-q} b$. Since $(g^t)^{-q}, b \in H$, $g^r \in H$. From the minimality of t, $r = 0$. So $b = g^{qt} = (g^t)^q \in \langle g^t \rangle$ and $H \subseteq \langle g^t \rangle$. Thus $H = \langle g^t \rangle$, a cyclic group.

Theorems for Cyclic Groups

(Ex.) In $\langle Z_6, + \rangle$,

$Z_6 = \{0,1,2,3,4,5\} = \{1^1, 1^2, 1^3, 1^4, 1^5, 1^6\}$

Subgroup $H = \langle 2 \rangle = \langle 1^2 \rangle = \{1^2, 1^4, 1^6\} = \{0,2,4\}$

Subgroup $S = \langle 3 \rangle = \langle 1^3 \rangle = \{1^3, 1^6\} = \{0,3\}$

$Z_6 = \{0,1,2,3,4,5\} = \{5^6, 5^5, 5^4, 5^3, 5^2, 5^1\} = \langle 5^1 \rangle$

Subgroup H $\langle 5^2 \rangle = \{5^2, 5^4, 5^6\}$

Subgroup S $\langle 5^3 \rangle = \{5^3, 5^6\}$

Lagrange Theorem

- **Lagrange's Theorem**

  If G is a finite group of order n with H a subgroup of order m, then m divides n.

- **Corollary 16.1**

  If G is a finite group and $a \in G$, then $ord(a)$ divides $|G|$.

- **Corollary 16.2**

  Every group of prime order is cyclic.

  There are only two types of subgroup, $\{e\}$ and G.

  For any $b\ (\neq e) \in G$, $\langle b \rangle = G$.

Example (1)

- In $\langle Z_{15}^*, \cdot \rangle$, $ord(2) = 4$ and $ord(4) = 2$.

a \ k	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	?						
14	14	1	14	1	14	1	14	1

Table of Powers, a^k

cyclic ?

$ab \bmod n = (a \bmod n)\, b \bmod n$

Example (2)

- In $\langle Z_{11}^*, \cdot \rangle$, $|Z_{11}^*| = 10$ cyclic ?

a \ k	1	2	3	4	5	6	7	8	9	10
1	(1)	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	(1)
3	3	9	5	4	(1)	3	9	5	4	1
4	4	5	9	3	(1)	4	5	9	3	1
5	5	3	4	9	(1)	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	(1)
7	7	5	2	3	10	4	6	9	8	(1)
8	8	9	6	4	10	3	2	5	7	(1)
9	9	4	3	5	(1)	9	4	3	5	1
10	10	(1)	10	1	10	1	10	1	10	1

Table of Powers, a^k

Example (3)

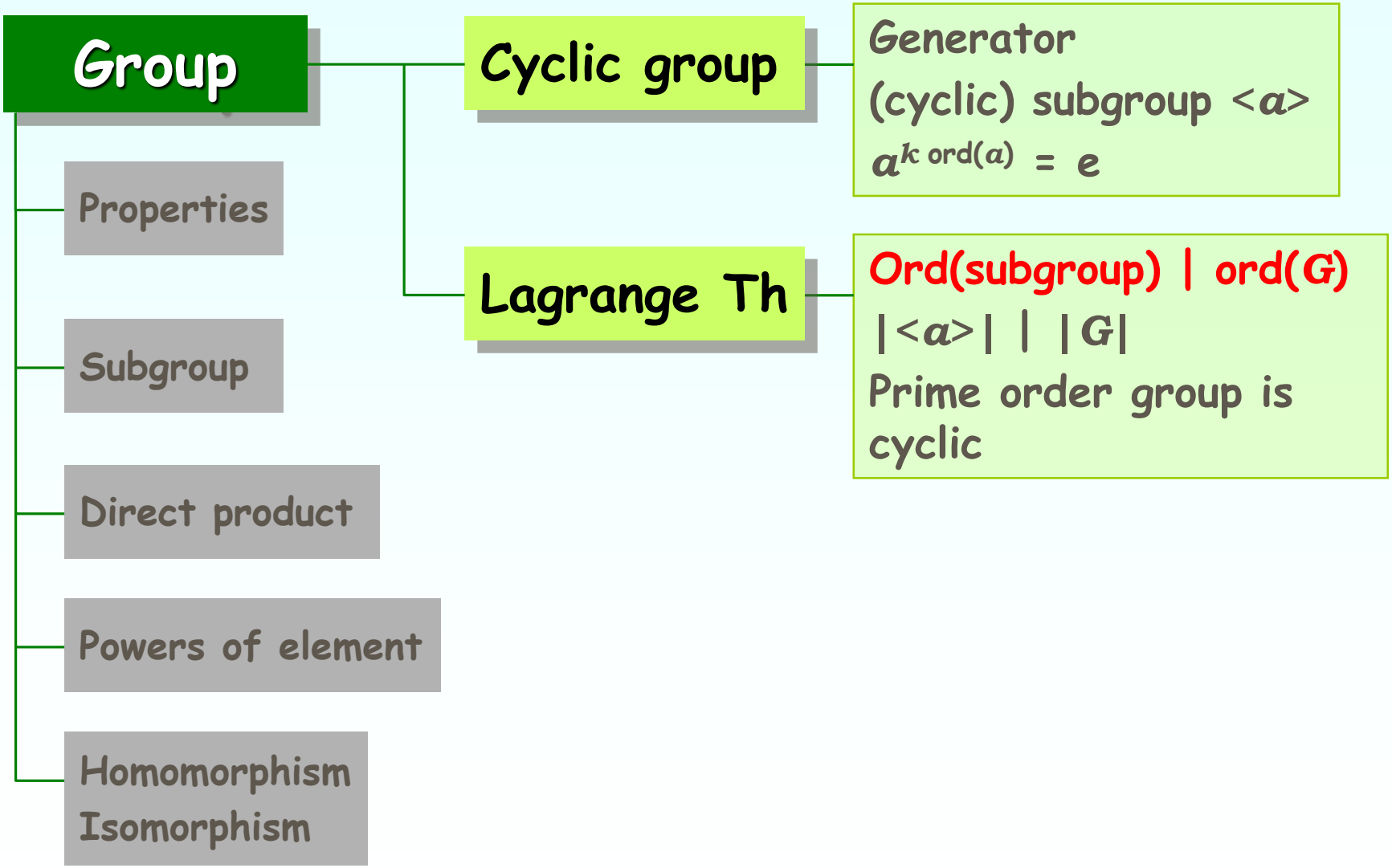
- In $\langle Z_5, + \rangle$, $|Z_5| = 5$

  Note that the number 5 is prime.

a \ k	1	2	3	4	5
0	0	0	0	0	0
1	1	2	3	4	0
2	2	4	1	3	0
3	3	1	4	2	0
4	4	3	2	1	0

Table of Powers, a^k

? ?


Group
Properties
Subgroup
Direct product
Powers of element
Homomorphism
Isomorphism
Cyclic group
Generator
(cyclic) subgroup <a>
$a^{k\,ord(a)} = e$
Lagrange Th
Ord(subgroup) | ord(G)
|<a>| | |G|
Prime order group is cyclic

Euler Theorem

- Euler Theorem

For each $n \in Z^+$, $n > 1$, and each $a \in Z$,
if $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

(Ex.1) If $n = 10$, $a = 3$, $\gcd(3,10)=1$, $\phi(10) = 4$,
then $a^{\phi(n)} = 3^4 = 81$ and $10 \mid (81 - 1)$.
When $a = -3$, $[(-3)^4] = [81] = [1]$.
When $a = 13$, $[13^4] = [28561] = [1]$.

(Ex.2) If $n = 5$, $a = 3$, $\gcd(3,5) = 1$, $\phi(5) = 4$,
then $[3^4] = [81] = [1]$. Similarly, $[2^4] = [16] = [1]$.

(Proof of Euler Th.)

(Lemma 1) A set $S = \{r_1,\ldots,r_{k(=\phi(n))}\}$ is called a reduced residue system mod n, where each r_i is relatively prime to n and $r_i \not\equiv r_j \bmod n$ for $i \neq j$.

If $\gcd(a,n) = 1$, then $\{ar_1,\ldots,ar_k\}$ is also a reduced residue system mod n.

We know that if $\gcd(a,n) = 1$ and $\gcd(b,n) = 1$ then $\gcd(ab,n) = 1$. Thus $\gcd(ar_i,n) = 1$, $i = 1,\ldots,k$.

Assume that $ar_1,\ldots,ar_k \pmod n$ are not distinct. Let $ar_i \equiv ar_j \bmod n$ for some $i \neq j$. Then $n \mid (ar_i - ar_j)$, that is, $n \mid a(r_i - r_j)$. If $\gcd(a,n) = 1$, then $r_i \equiv r_j \bmod n$.

This contradicts distinctness of $r_1,\ldots,r_k \pmod n$. Thus $ar_1,\ldots,ar_k \pmod n$ are distinct. □

(Proof of Euler Th.)

(Lemma 2) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$.

For some $i, j \in Z$, $a = b+in$ and $c = d+jn$. Then $ac = (b+in)(d+jn) = bd+n(bj+di+ijn)$. Thus $ac \equiv bd \bmod n$. □

Let $\{r_1,\ldots,r_{k(=\phi(n))}\}$ be a reduced residue system mod n.

If $\gcd(a,n) = 1$, from Lemma 1, $\{ar_1,\ldots,ar_k\}$ is also a reduced residue system mod n.

Thus there exists a unique r_j such that $ar_i \equiv r_j \bmod n$. Then

$r_1\cdots r_k \equiv ar_1\cdots ar_k \bmod n$ (from Lemma 2)

$\Rightarrow r_1\cdots r_k \equiv a^{\phi(n)}r_1\cdots r_k \bmod n \Rightarrow n \mid (1-a^{\phi(n)})\, r_1\cdots r_k$

We know that $\gcd(r_1\cdots r_k,n) = 1$.

Thus $a^{\phi(n)} \equiv 1 \bmod n$ ■

(Proof of Euler Th.)

$n = 10$, $S = \{1,3,7,9\}$

$a = 3$ ➔ $\{3,9,21,27\}$ is a reduced system mod 10

gcd(3,10)=gcd(9,10)=gcd(21,10)=gcd(27,10)=1

The elements are not congruent to modulo 10 each other

$1 \cdot 3 \cdot 7 \cdot 9 \equiv 3 \cdot 9 \cdot 21 \cdot 27 \bmod 10$

How about $a = 11$?

$\Rightarrow 1 \cdot 3 \cdot 7 \cdot 9 \equiv 3^{\phi(10)} \cdot 1 \cdot 3 \cdot 7 \cdot 9 \bmod 10$

$\Rightarrow 10 \mid (1 - 3^{\phi(10)}) \cdot 1 \cdot 3 \cdot 7 \cdot 9$

$\Rightarrow 3^{\phi(10)} \equiv 1 \bmod 10$

because $\gcd(10, 1 \cdot 3 \cdot 7 \cdot 9) = 1$

Euler Theorem

- **Euler Theorem**

  For each $n \in Z^+$, $n > 1$, and each $a \in Z$,
  if $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

For any integer $n > 1$,
$a^{\phi(n)} \equiv 1 \bmod n$ for all $a \in Z_n^*$.

(Note) Z_n^* is a multiplicative group of order $\phi(n)$.

Lagrange theorem
$\phi(n) = k\ ord(a)$

$$a^{\phi(n)} = a^{k\ ord(a)}$$
$$= (a^{ord(a)})^k = e^k = 1$$

Example

- In $<Z_{15}^{*}, \cdot>$, $a^{\phi(n)} \equiv 1 \bmod n$

$\phi(15) = 8$

a \ k	1	2	3	4	5	6	7	8
1	(1)	1	1	1	1	1	1	1
2	2	4	8	(1)	2	4	8	1
4	4	(1)	4	1	4	1	4	1
7	7	4	13	(1)	7	4	13	1
8	8	4	2	(1)	8	4	2	1
11	11	(1)	11	1	11	1	11	1
13	13	4	7	(1)	13	4	7	1
14	14	(1)	14	1	14	1	14	1

Table of Powers, a^k

cyclic ?

Fermat Theorem

- **Fermat's Little Theorem**

  If p is prime, $a^p \equiv a \bmod p$ for each $a \in Z$.

  (Proof)

  If $\gcd(a,p) = 1$, then $a^{\phi(p)} \equiv 1 \bmod p$ by Euler theorem. Since $\phi(p) = p-1$, $a^{p-1} \equiv 1 \bmod p$ and thus $a^p \equiv a \bmod p$.

  If $\gcd(a,p) \neq 1$, then $a = kp$ for some $k \in Z$.

  Since $a^p - a = a(a^{p-1}-1) = (kp)(a^{p-1}-1)$, $p \mid (a^p - a)$.

  Thus $a^p \equiv a \bmod p$.

  If p is prime, $a^p \equiv a \bmod p$ for all $a \in Z_p^*$.

Example

- In $<Z_{11}^*, \cdot>$, $a^{p-1} \equiv 1 \bmod p$ & $a^p \equiv a \bmod p$

$\phi(11) = 10$

a^k	1	2	3	4	5	6	7	8	9	10	11
1	(1)	1	1	1	1	1	1	1	1	1	
2	2	4	8	5	10	9	7	3	6	(1)	
3	3	9	5	4	(1)	3	9	5	4	1	
4	4	5	9	3	(1)	4	5	9	3	1	
5	5	3	4	9	(1)	5	3	4	9	1	
6	6	3	7	9	10	5	8	4	2	(1)	
7	7	5	2	3	10	4	6	9	8	(1)	
8	8	9	6	4	10	3	2	5	7	(1)	
9	9	4	3	5	(1)	9	4	3	5	1	
10	10	(1)	10	1	10	1	10	1	10	1	

Table of Powers, a^k

Generators in Z_p^*

- **Theorem**

  If p is prime, Z_p^* is a cyclic group of order $p-1$.
  The number of generators for Z_p^* is $\phi(p-1)$.

(Proof)

(Lemma 3) Let a and b be elements of an abelian group G, of finite orders u and v, respectively. Then G contains an element of order $\text{lcm}(u,v)$.

(Ex.) In the group Z_{11}^*, there are elements of orders 2 and 5. Thus Z_{11}^* contains an element of order 10.

Generators in Z_p^*

Let m be the least common multiple (lcm) of the orders of elements of the abelian group Z_p^*.

From induction of Lemma 3, Z_p^* contains an element of order m. Then m divides the order of Z_p^*, $p-1$, from Lagrange theorem. Thus $m \leq p-1$.

Meanwhile, the order of every element divides m. Notice that $a^k \equiv 1 \bmod p$ for an element a of order k. *Thus every element is a root of the field polynomial* $x^m - 1$. Since this polynomial has at most m roots, $p-1 \leq m$.

Therefore $p-1 = m$, and Z_p^* contains an element of order $p-1$. It is a cyclic group.

$a^m = a^{kc} = (a^k)^c = (1)^c = 1$ at the field $<Z_p, +, \cdot>$

Generators in Z_p^*

(Lemma 4) If h is the order of an element a in a group, that is, $a^h = e$, then the element a^k has order $h / \gcd(h, k)$.

Let g be a generator of Z_p^*. Then its order is $p-1$.

Subgroup $<g>$ can be written as $\{g^1, g^2, \ldots, g^{p-1}\}$.

From Lemma 4, we see that only the element g^k with $\gcd(p-1, k) = 1$ has order $p-1$.

Thus the number of generators for Z_p^* is $\phi(p-1)$. ■

(Ex.) In Z_{11}^*, there are $\phi(10) = 4$ generators.

- Generators : 2, 6, 7, 8

Example

$\gcd(k,10) \neq 1 \Rightarrow$ not generator

$\text{ord}(g^k) = 10/\gcd(k,10) \therefore \phi(10) = 4$

- In $<Z_{11}^*, \cdot>$, $\phi(p-1) = 4$

a^k	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Table of Powers, a^k

An Example for Lemma 4

- In $<Z_{11}^{*}, \cdot>$, $Ord(2^8) = 10/gcd(10,8) = 5$

  $Ord(2^5) = 10/gcd(10,5) = 2$

  $Ord(4^3) = 5/gcd(5,3) = 5$

a^k	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

An Example for Lemma 4

- In $<Z_{15}^{*}, \cdot>$, $Ord(7^3) = 4/gcd(4,3) = 4 = Ord(13)$

  $Ord(7^6) = 4/gcd(4,6) = 2 = Ord(4)$

  $Ord(2^3) = 4/gcd(4,3) = 4 = Ord(8)$

a^k	1	2	3	4	5	6	7	8
1	(1)	1	1	1	1	1	1	1
2	2	4	8	(1)	2	4	8	1
4	4	(1)	4	1	4	1	4	1
7	7	4	13	(1)	7	4	13	1
8	8	4	2	(1)	8	4	2	1
11	11	(1)	11	1	11	1	11	1
13	13	4	7	(1)	13	4	7	1
14	14	(1)	14	1	14	1	14	1

cyclic ?

(Proof of Lemma 3)

(Proof) We know that $a^u = 1$ and $b^v = 1$. Let $m = \text{lcm}(u,v)$.

Case 1: $\gcd(u,v) = 1$. Then $m = uv$. Since G is abelian, $(ab)^m = (ab)^{uv} = (a)^{uv}(b)^{uv} = (a^u)^v (b^v)^u = 1^v 1^u = 1$. Thus $r = \text{ord}(ab)$ divides m. Conversely $(ab)^r = 1 = (ab)^{ru} = (a^u)^r b^{ru} = b^{ru}$. Thus $v|ru \Rightarrow v|r$, since $\gcd(u,v) = 1$. Similarly $u|r$. Then $uv|r$. That is, $m \mid \text{ord}(ab)$. Thus $\text{ord}(ab) = m$. Therefore G contains the element ab of order $\text{lcm}(u,v)$.

Case 2: $\gcd(u,v) = d > 1$. Let l be a prime that divides d, and let $u' = u/l$, $v' = v/l$, and $d' = d/l$. Then $d' = \gcd(u',v')$, so d cannot divide both of u' and v'. Let us say that d does not divide u'. Then $\gcd(u',v) = d'$, and $\text{lcm}(u',v) = u'v/d' = uv/d = m$. Since a has order u, a^l has order $u/l = u'$. We replace the pair of elements a,b by the pair a^l,b. This has the effect of replacing u, v, d, and m by u', v, d', and m, respectively. The gcd has been decreased while keeping the lcm constant. Induction on d completes the proof.

(Proof of Lemma 4)

(Proof of Lemma 4)

$(a^k)^j = e$

$\Leftrightarrow a^{kj} = e$

$\Leftrightarrow h \mid kj$

$\Leftrightarrow h / \gcd(h,k) \mid (k / \gcd(h,k))\, j$ — $h / \gcd(h,k)$ and $k / \gcd(h,k)$ are relatively prime

$\Leftrightarrow h / \gcd(h,k) \mid j$

The smallest such positive $j = h / \gcd(h,k)$.
Therefore a^k has order $h / \gcd(h,k)$.

Let $a^{\mathrm{ord}(a)} = a^h = e$ for $a \in$ a group G.
What is the smallest positive j such that $(a^k)^j = e$?

Discrete Logarithm

- **Definition**

  Let g be a fixed generator for Z_p^*.

  Each $a \in Z_p^*$ has associated with it a unique integer $r \in \{0, 1, \ldots, p-2\}$ such that

  $$a \equiv g^r \bmod p$$

  This r is denoted by $ind_{p,g}(a)$ and is called the index of a with respect to p, g.

Example

- For $g = 2$ in $\langle Z_{11}^*, \cdot \rangle$,

$2^3 \bmod 11 = 8$

$ind_{11,2}(8) = 3$

$2^5 \bmod 11 = 10$

$ind_{11,2}(10) = 5$

$2^{10} \bmod 11 = 1$

$ind_{11,2}(1) = 0$

Unique index

a^r	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Table of Powers, a^r

Discrete Log Problem

- **Definition**

  Given p, g, a, computing $ind_{p,g}(a)$ is called the *discrete log problem*.

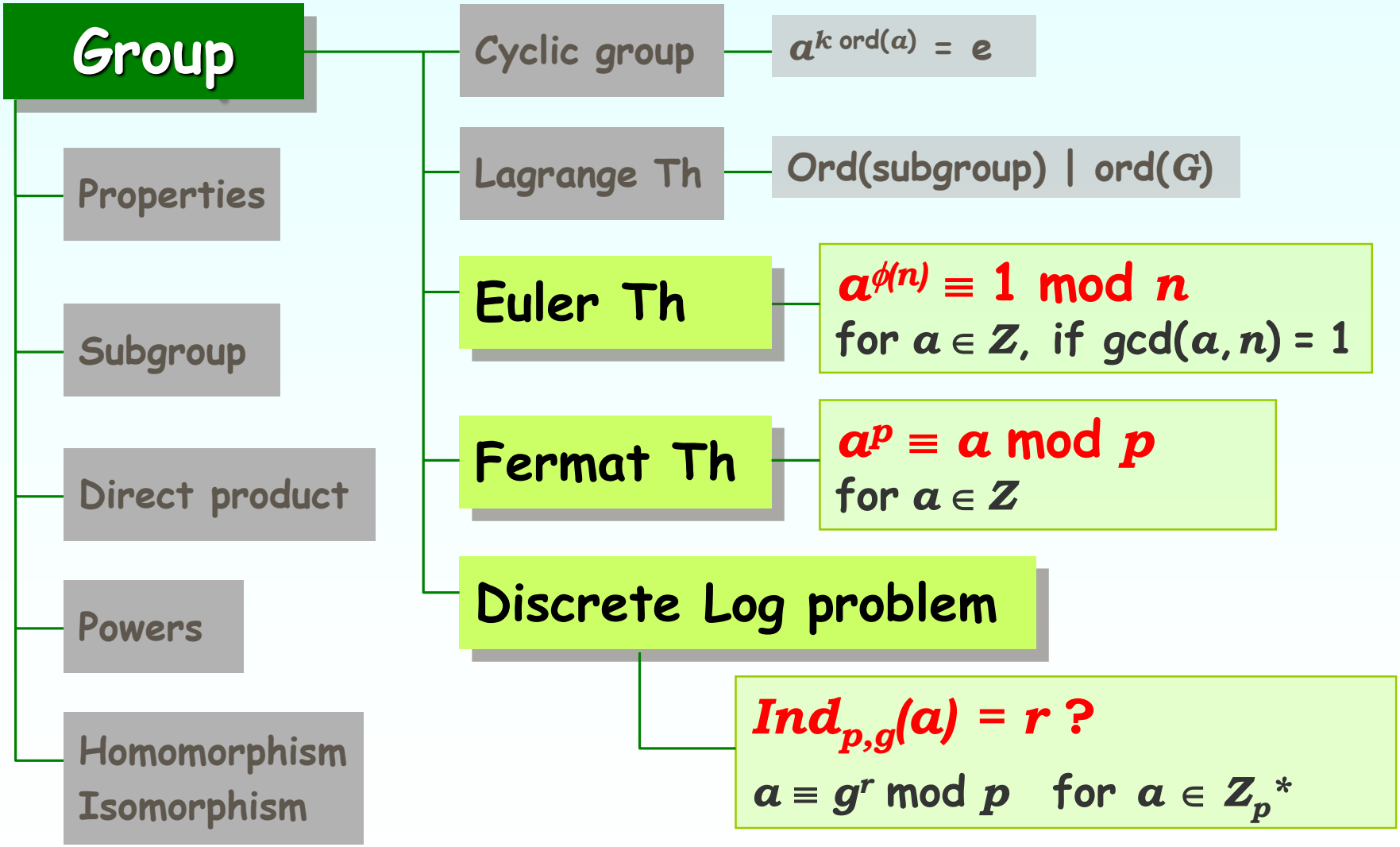
  It is an open problem

  whether the discrete log problem can be solved in deterministic polynomial time.

$$a + kp = g^r, \quad 1 \le a < p, \ 0 \le r \le p-2$$

$$r = \log_g (a + kp)$$

? ? ?


Group
Properties
Subgroup
Direct product
Powers
Homomorphism
Isomorphism
Cyclic group
$a^{k\,\mathrm{ord}(a)} = e$
Lagrange Th
Ord(subgroup) | ord(G)
Euler Th
$a^{\phi(n)} \equiv 1 \bmod n$
for $a \in Z$, if $\gcd(a, n) = 1$
Fermat Th
$a^p \equiv a \bmod p$
for $a \in Z$
Discrete Log problem
$Ind_{p,g}(a) = r$?
$a \equiv g^r \bmod p$ for $a \in Z_p^*$

응용1: Diffie-Hellman's Key Exchange

- Diffie-Hellman's Protocol
  - The first to use the Discrete Log Problem
  - Share a secrete key in insecure networks
- 공개 정보
  - A large prime p, a generator g

y_A

y_B

A비밀키: X_A

$y_A = g^{X_A} \bmod p$

공유키 K 생성 완료

$K = g^{X_A X_B} \bmod p$

B비밀키: X_B

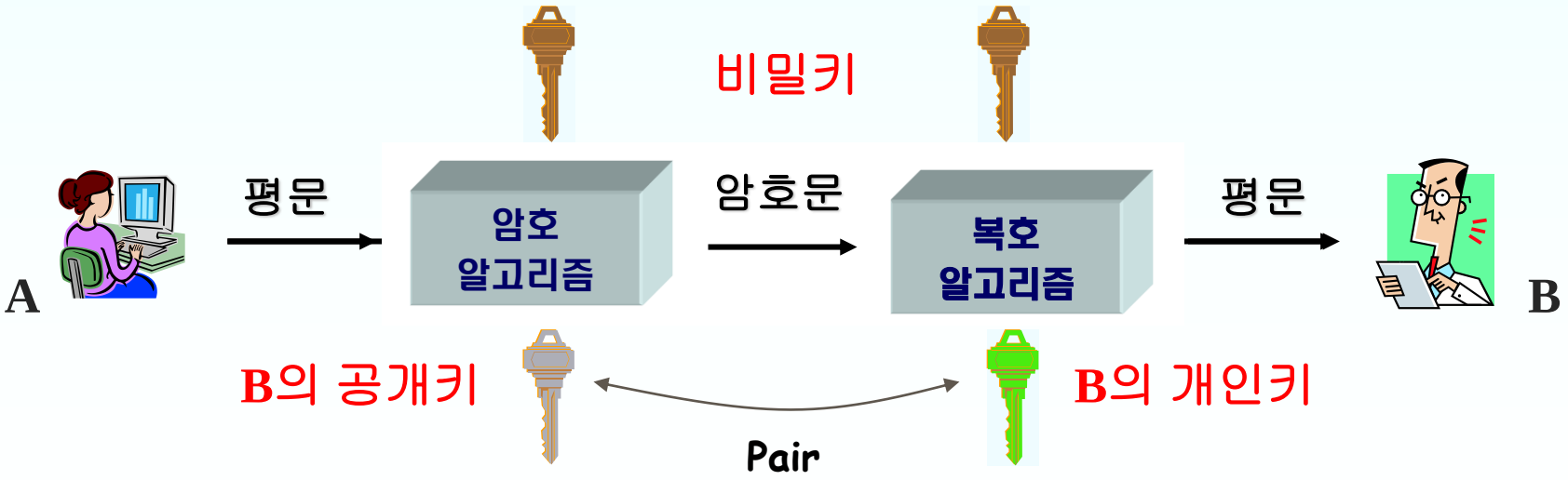
$y_B = g^{X_B} \bmod p$

$y_B^{X_A} \bmod p = g^{X_B X_A} \bmod p$

$y_A^{X_B} \bmod p = g^{X_A X_B} \bmod p$

응용2: ElGamal Cryptosystem

- Types of Cryptosystem
  - Private-key cryptosystem
    - DES, IDEA, AES, etc
  - Public-key cryptosystem
    - RSA, ElGamal, ECC, etc



응용2: ElGamal Cryptosystem

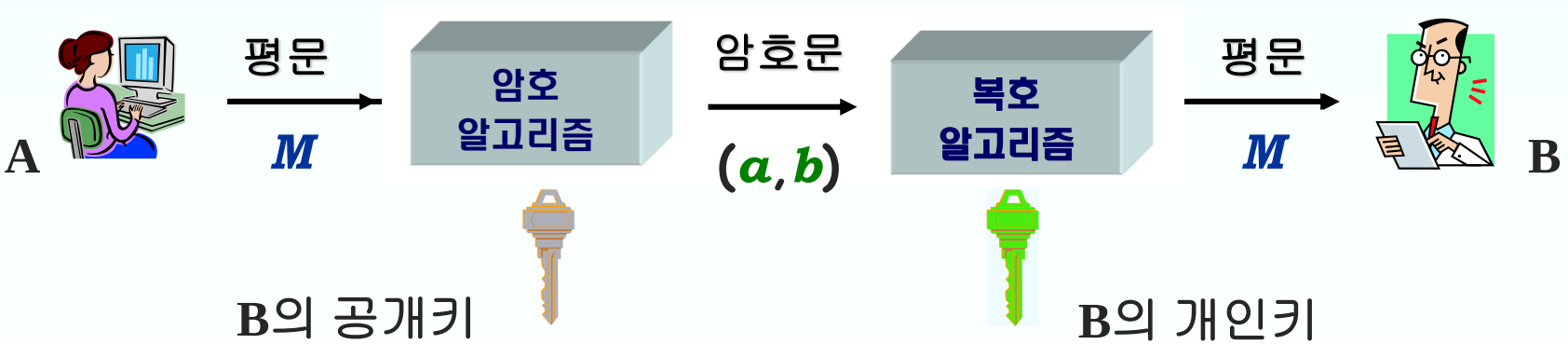
- ElGamal Algorithm
  - Discrete Log Problem의 어려움에 근거
  - Digital signature, encryption 에서 사용

(k: 난수)

$a = g^k \bmod p$

$b = y^k M \bmod p$

$M = b/a^x \bmod p$



B의 공개키

p, g, y (= $g^x \bmod p$)

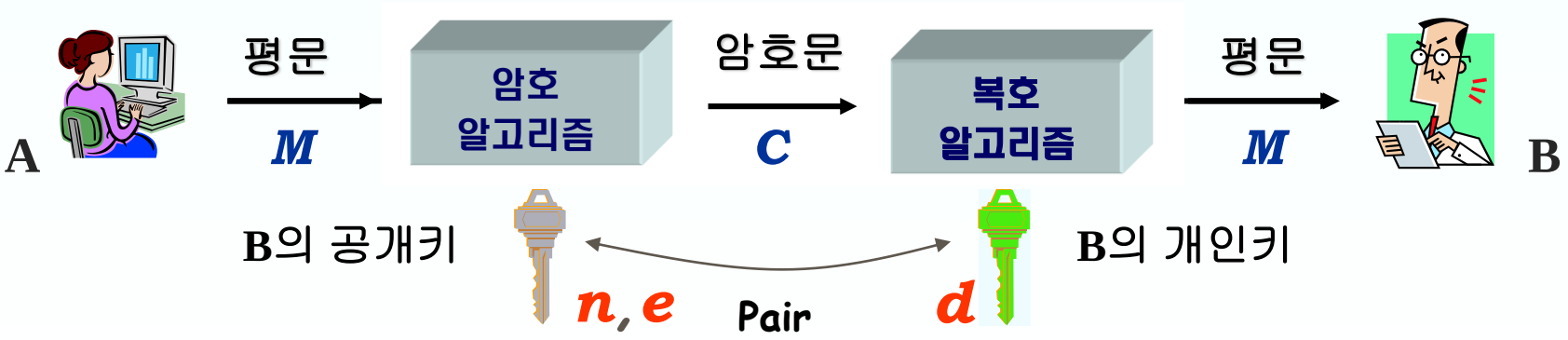
B의 개인키

x

응용3: RSA Cryptosystem

- RSA public-key cryptosystem
  - 1978년, MIT의 Rivest, Shamir, Adleman
  - Factoring (소인수분해) 어려움에 근거
  - 시스템 구성
    - 공개키: $n\ (= pq),\ e$ 개인키: d
  - 암호화 : $E(M) = M^e \bmod n = C$

    복호화 : $D(C) = C^d \bmod n = M$



응용3: RSA Cryptosystem

- For two distinct primes p, q, $n = pq$, $r = \phi(n)$
- Select e ($\gcd(e, r) = 1$) and its inverse d ($= e^{-1}$)
- $E(M) = M^e \bmod n = C$
  $D(C) = C^d \bmod n = M$

(note) $e \in Z_r^*$

(Ex) $p = 61$, $q = 127$, $n = 7747$, $r = (p-1)(q-1) = 7560$,
$e = 17$, $d = 3113$, $M = 2104$

$2104^{17} \bmod 7747 = 0628$

$0628^{3113} \bmod 7747 = 2104$

$d \leftarrow$ Ext-Euclid(r, e)

응용3: RSA Cryptosystem

Correctness of RSA

$$
\begin{aligned}
D(C) &= C^d \bmod n \\
&= (M^e)^d \bmod n \\
&= M^{ed} \bmod n && ; \gcd(e, r) = 1,\ d = e^{-1} \\
&= M^{k\phi(n)+1} \bmod n \\
&= M \bmod n && \gcd(M, n) = 1\ ?
\end{aligned}
$$

- $ed \equiv 1 \bmod r$ in Z_r^*. Thus $ed = kr + 1 = k\phi(n) + 1$
- (Euler theorem) For each $n \in Z^+$, $n > 1$, and each $a \in Z$, if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

응용3: RSA Cryptosystem

Correctness of RSA

- If $\gcd(M,n) = 1$, then $M^{\phi(n)} \equiv 1 \bmod n$.

  $\gcd(M,n) = 1$? → Not perfect

- Fail probability
  $= 1-[\phi(n)/n]$
  $= 1-(p-1)(q-1)/pq$
  $= (1/p) + (1/q) - (1/pq)$

응용3: RSA Cryptosystem

- Security of RSA
  - If we could compute r (= $\phi(n)$ = $(p-1)(q-1)$) from the given public-key (n, e), the decryption key d can be determined
    - Note that $d = e^{-1}$ in Z_r^* $\quad d \leftarrow$ Ext-Euclid(r, e)
  - Computing problem of r is derived to determining of p and q
  - The p and q are 100 or more digits long

응용3: RSA Cryptosystem

- **A Practical Issue**
  - **How to compute a^e mod n in real time**

```
Procedure Modular Exponentiation (a: integer;
                  n, e = (b_m b_{m-1} … b_1 b_0)_2 : positive integer)
begin
   x := 1
   power := a mod n
   for i = 0 to m do
      begin
         if b_i = 1 then x := (x * power) mod n
         power := (power * power) mod n
      end
end
```

응용3: RSA Cryptosystem

(Ex.) $5^{23} \bmod 64$ ($23 = 010111_2$)

$5^{23} = 5^{(010111)_2} = 5^{16+4+2+1} = 5^{16}.5^{4}.5^{2}.5^{1} \pmod{64}$

$5^1 : 5 \bmod 64 = 5$	$1 \cdot 5 \bmod 64 = 5$
$5^2 : 5^2 \bmod 64 = 25$	$5 \cdot 25 \bmod 64 = 61$
$5^4 : 25^2 \bmod 64 = 49$	$61 \cdot 49 \bmod 64 = 45$
$5^8 : 49^2 \bmod 64 = 33$	
$5^{16} : 33^2 \bmod 64 = 1$	$45 \cdot 1 \bmod 64 = 45$
$5^{32} : 1^2 \bmod 64 = 1$