Modern Applied Algebra

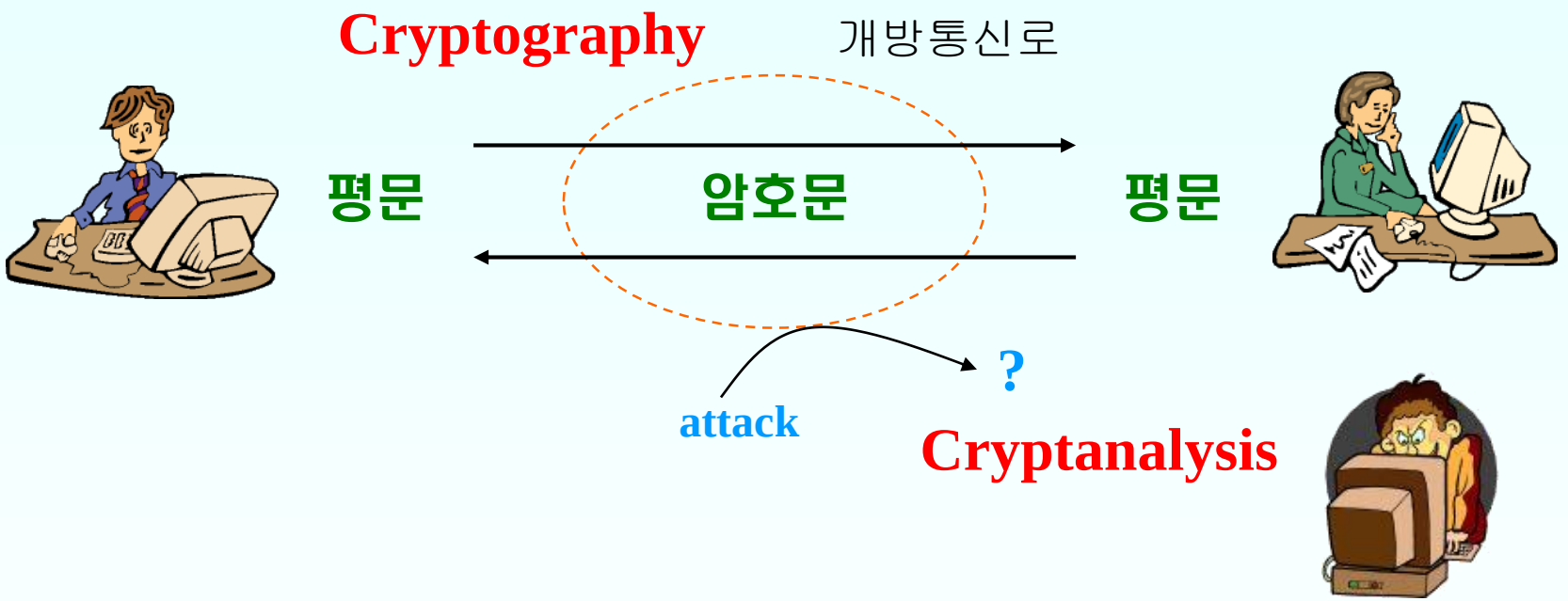
- Group, Ring, Field

부산대학교
PUSAN NATIONAL UNIVERSITY

Overview

1. Algebra
   - Definition of Group, Ring, Field (14.1, 16.1)
2. Integer modulo N
   - 14.3
3. Group Properties and Applications
   - 16.1-2, 16.4
4. Ring and Field Properties
   - 14.2, 14.4
5. Polynomial Ring and Finite Field
   - 17.1-2

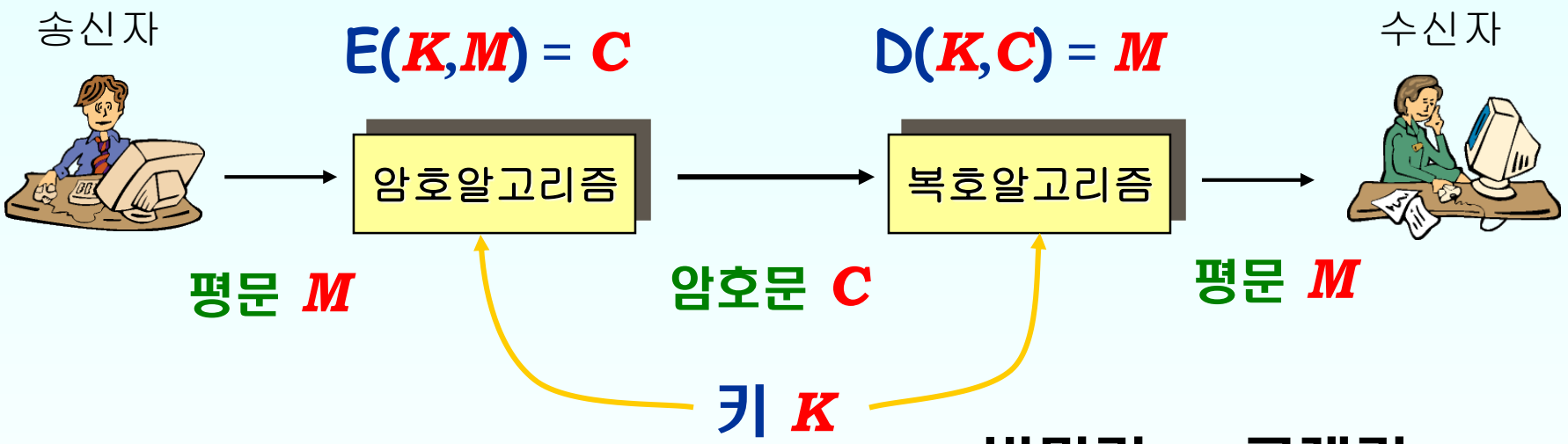
Cryptology (암호학)



암호학 = 암호작성 + 암호해독

- 암호작성 (cryptography) : code making
- 암호해독 (cryptanalysis) : code breaking

암호시스템 구성



비밀키 vs 공개키

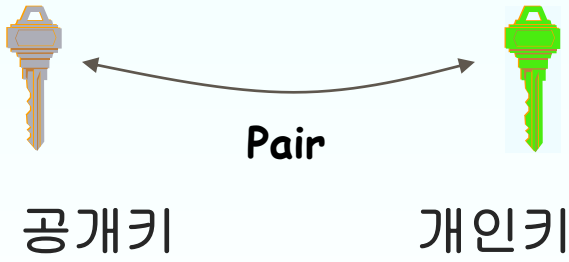
기본 조건

- E(K,M) 과 D(K,C)의 계산은 쉬워야 된다
- K를 모를 때 C에서 M을 계산하는 것은 어려워야 된다

암호 시스템 종류

- 비밀키 (private key) 방식
  - 암호키 = 복호키, 키 전달 문제
  - 대칭키, 단일키 방식
  - DES, IDEA, AES (Rijndael)
  - Galois Field GF(2^n) 이해 필요

- 공개키 (public key) 방식
  - 암호키 ≠ 복호키
  - RSA, ElGamal, ECC
  - Prime Number, Discrete Log Problem, Euler Theorem, Fermat Theorem 등의 이해 필요



Basic Properties and Def. of Group, Ring, Field

부산대학교
PUSAN NATIONAL UNIVERSITY

Algebra

- Algebra Definition
  - Tuple $< K, op_1, op_2, \ldots, op_n >$
    - $< R, +, -, \times, \div >$
    - $< \{T,F\}, \wedge, \vee, \neg >$; Boolean algebra
- K : a set of data
  - $|K|$: order of the algebra
  - finite or infinite
- Operators op_j
  - Closed $op_j : K^i \rightarrow K$
    - Unary if $i = 1$, Binary if $i = 2$, …

K^2 or $K \times K$: Cartesian Product

Identity and Zero Elements

- $\oplus : K \times K \rightarrow K$

  Identity element (항등원) e for $\oplus$ in K

  - $e \oplus a = a \oplus e = a$ for all $a \in K$

  Zero element (영원) z for $\oplus$ in K

  - $z \oplus a = a \oplus z = z$ for all $a \in K$

Examples

$< Z, + >$

- Identity : 0, Zero : none

$< Z, \times >$

- Identity : 1, Zero : 0

Inverse

- $\oplus : K \times K \rightarrow K$

  Let e be the identity element for $\oplus$ in K

  - Left inverse
    - $a'_L \oplus a = e \, , \, a \in K$
  - Right inverse
    - $a \oplus a'_R = e \, , \, a \in K$
  - If $a'_L = a'_R = a'$, a' is the inverse of a

Example $< Z, + >$

- Identity 0
- (-x) is the inverse of x : x + (-x) = (-x) + x = 0

Associative and Commutative

- $\oplus : K \times K \rightarrow K$

  The operator $\oplus$ is associative, when

  - $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for all $a, b, c \in K$

  The operator $\oplus$ is commutative, when

  - $a \oplus b = b \oplus a$ for all $a, b \in K$

Examples

$< Z, + >$ and $< Z, \times >$

- Associative and Commutative

Algebra (with one binary operator)

$< K, \oplus >$

A closed binary operator $\oplus : K \times K \rightarrow K$

Semigroup (반군) : Associative

- $< Z^+, + >$

Monoid (단위반군) : Associative, Identity

- $< N, + >$, $< Z, \times >$, $< \{T,F\}, \wedge >$

Group (군) : Associative, Identity, Inverse

- $< Z, + >$

Abelian group (대수군) :

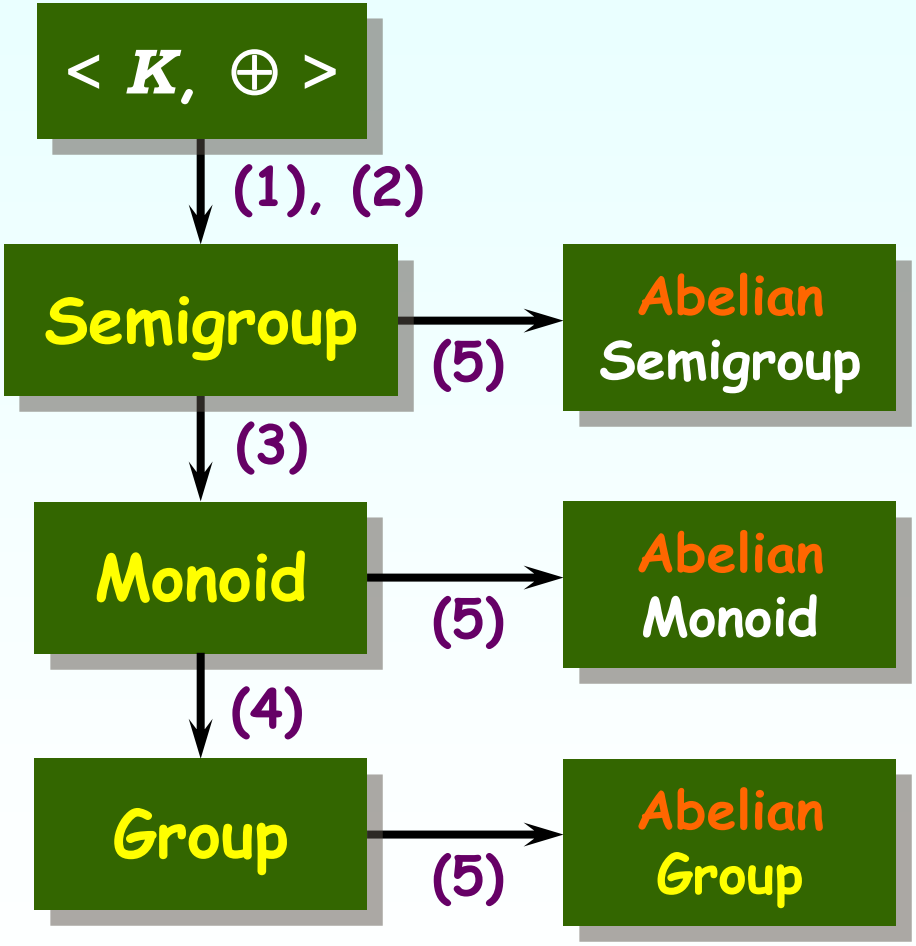
Associative, Identity, Inverse, Commutative

- $< Z, + >$

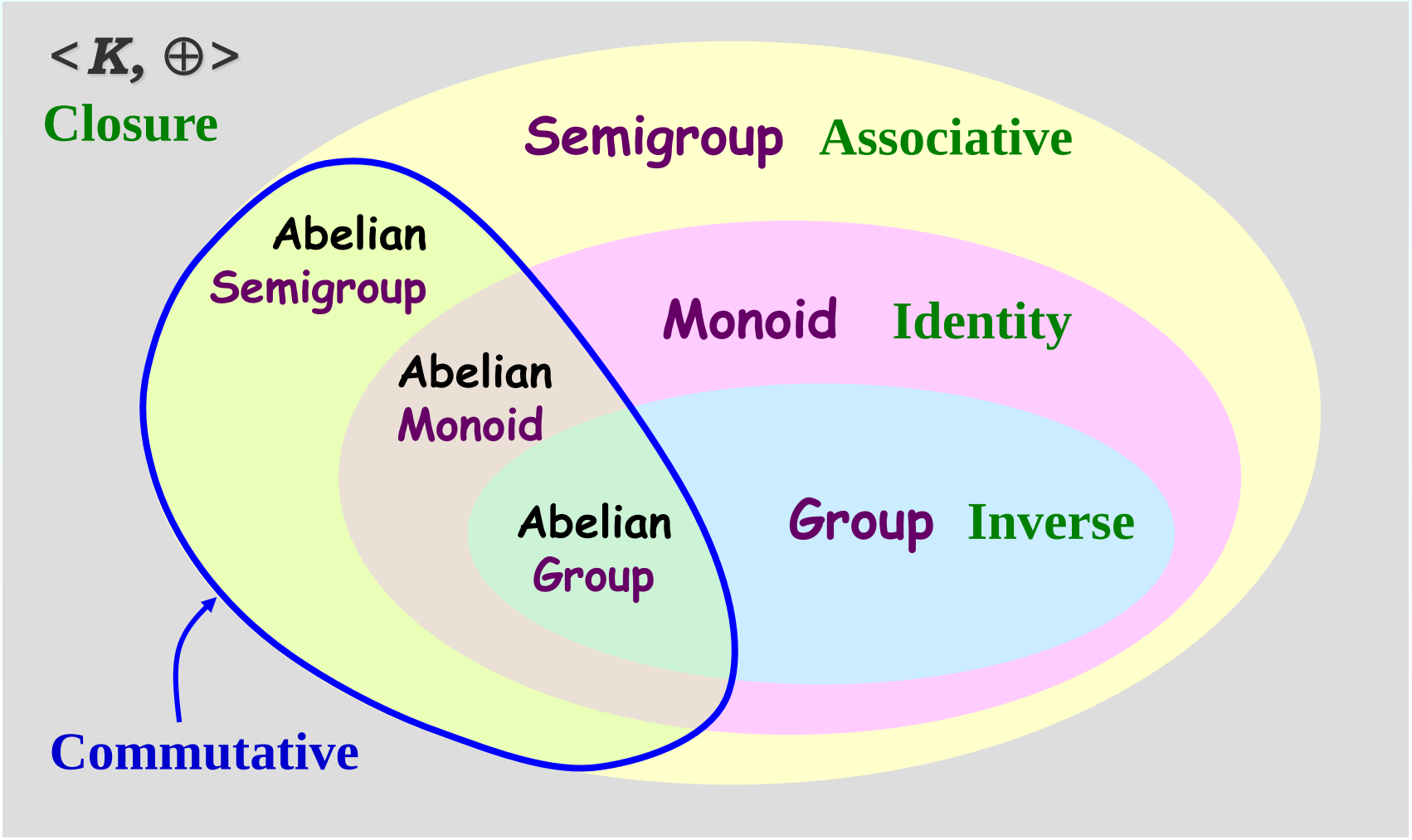
Algebra (with one binary operator)

Properties

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



Algebra (with one binary operator)



Algebra (with two binary operators)

$< K, \oplus, \otimes >$

Two closed binary operators : $K \times K \rightarrow K$

$\oplus$ additive operator
$\otimes$ multiplicative op.

- **Ring** $< K, \oplus, \otimes >$
  - $< K, \oplus >$ is an abelian group.
  - $\otimes$ is distributive over $\oplus$
    - $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ and
    - $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

      for all $a, b, c \in K$.
  - $\otimes$ is associative

Algebra (with two binary operators)

$< K, \oplus, \otimes >$

$< K, \oplus >$: abelian group, and distribution laws hold

❖ Conditions for $\otimes$ ⇐

Ring (환) : Associative

Ring with Unity : Associative, Identity

Commutative Ring : Associative, Commutative

Commutative Ring with Unity

Associative, Identity, Commutative

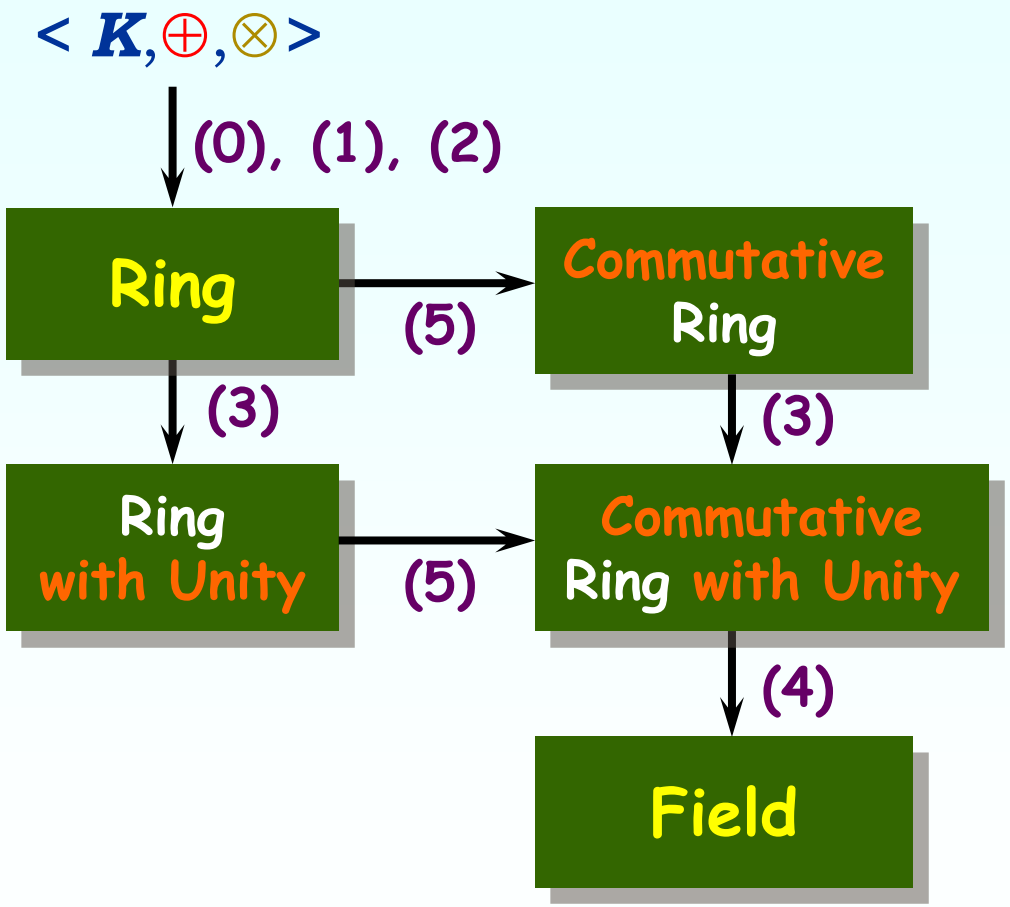
Field (체)

Associative, Identity, Commutative, Inverse

Algebra (with two binary operators)

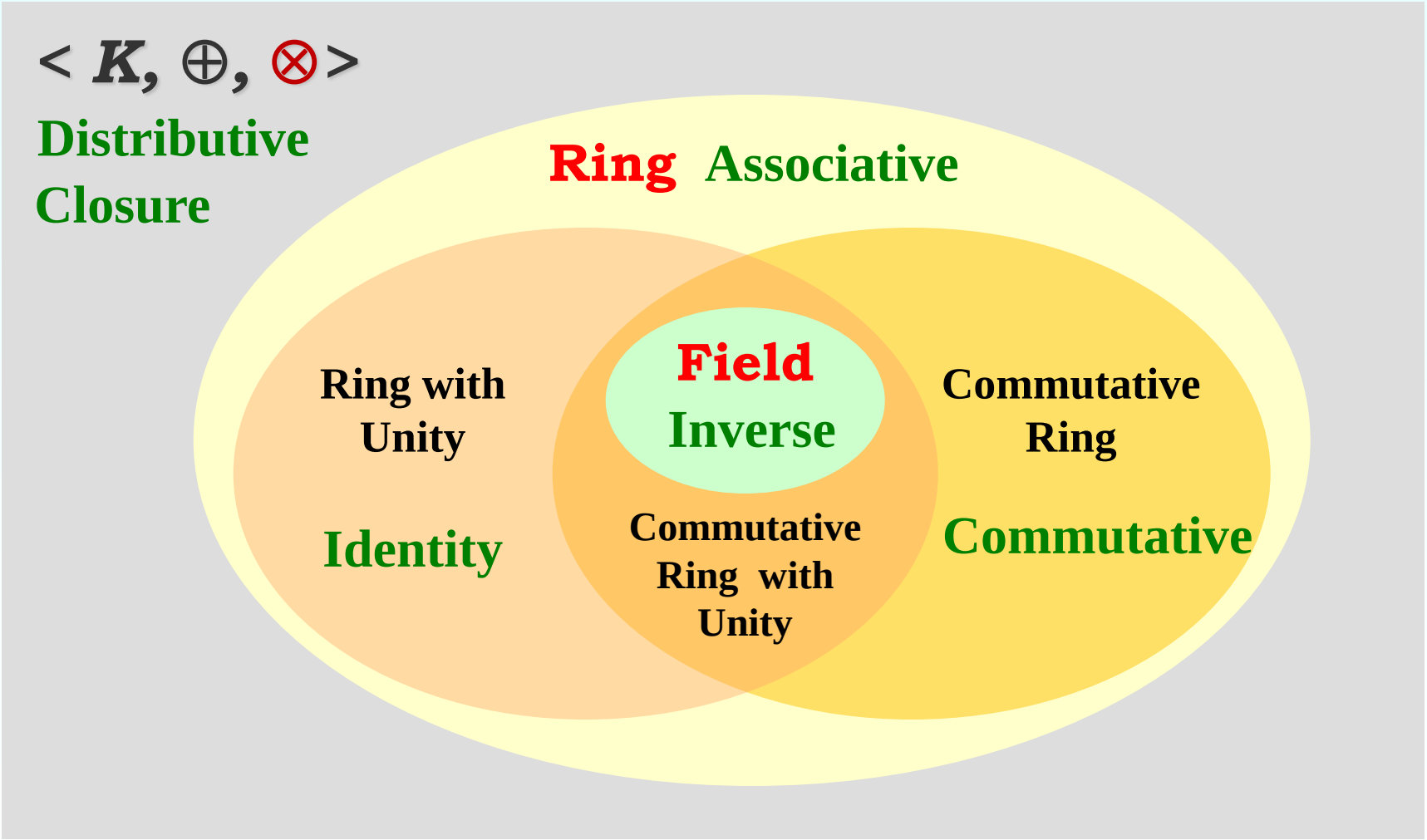
Properties for ⊗

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



(Note) Inverse for ⊗
Not defined for zero element (= additive identity)

Algebra (with two binary operators)



Example: Square Matrix

- $< M, \oplus, \otimes >$

  M : a set of $n \times n$ matrix

  $\oplus$: ordinary matrix addition

  $\otimes$: ordinary matrix multiplication

  Distributive $\otimes$ over $\oplus$

- $< M, \oplus >$

  Closure, Associative, Identity (zero matrix),

  Inverse, Commutative ➔ **Abelian Group**

- $< M, \otimes >$

  Closure, Associative, Identity

  Not Commutative, Not Inverse

Example: Ring and Field

- Rings for $< K, \oplus, \otimes >$
  - $\oplus$: ordinary addition
  - $\otimes$: ordinary multiplication
  - K : 정수, 유리수, 실수 , 복소수
    - $< Z, +, \cdot >$, $< Q, +, \cdot >$, $< R, +, \cdot >$, $< C, +, \cdot >$
- Ring but not Field
  - $< Z, +, \cdot >$: Not Inverse for $\cdot$
- Field
  - $< Q, +, \cdot >$, $< R, +, \cdot >$, $< C, +, \cdot >$

(Note)
Inverse for $\otimes$

Defined for nonzero elements

(cf.) Vector Space in LA

- Vector Space in linear algebra
  - Focused on linear combination $ax + by + cz$
  - Addition axioms:
    - Closed, Commutative, Associative, Zero (Identity), Negative (Inverse)
  - Scalar Multiplication axioms:
    - Closed, two Distributives, Harmonious, One

Linear Indep., Basis, Dimension, Linear Trans., Orthogonality, Eigenvectors, SVD

(cf.) Boolean Algebra in DM(1)

- Boolean Algebra $(\mathcal{B}, +, *, \neg, 0, 1)$ in DM(1)
  - Focused on logic operation
    - → Switching theory, Set theory
      - Closed op's, two Commutative op's, two Distributives, two Identities, Inverse law

a) $x + y = y + x \quad x * y = y * x$ commutative laws

b) $x * (y + z) = (x * y) + (x * z)$

$x + (y * z) = (x + y) * (x + z)$ distributive laws

c) $x + 0 = x \quad x * 1 = x$ identity laws

d) $x + \bar{x} = 1 \quad x * \bar{x} = 0$ inverse laws

e) $0 \neq 1$