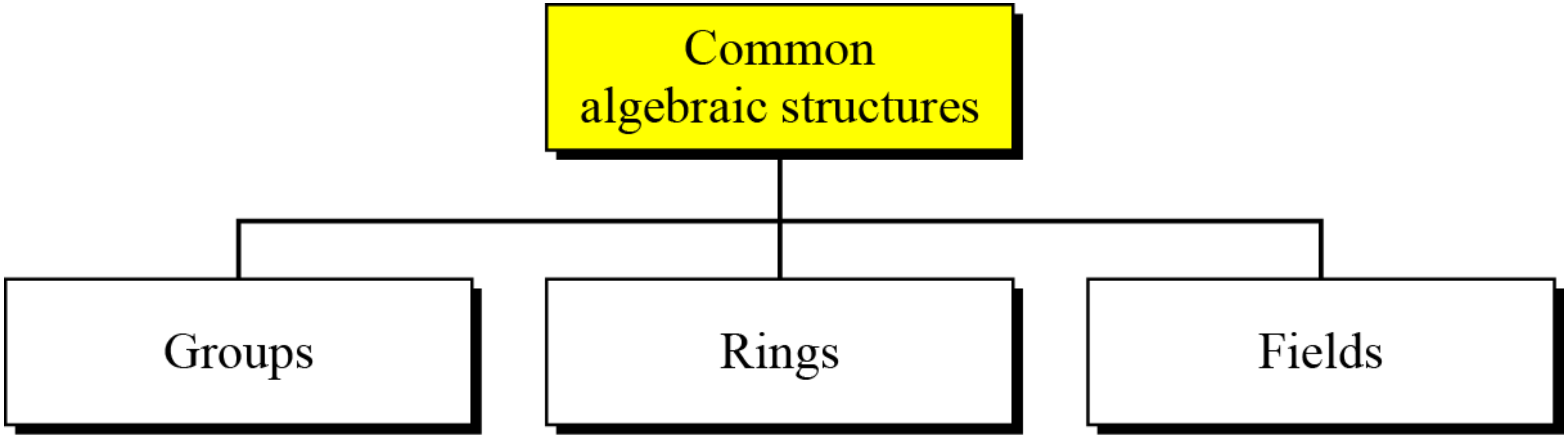
ALGEBRAIC STRUCTURES

ALGEBRAIC STRUCTURES

Cryptography requires sets of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure*. In this chapter, we will define three common algebraic structures: groups, rings, and fields.*

Common Algebraic Structure



Groups

A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms). A commutative group satisfies an extra property, commutativity:

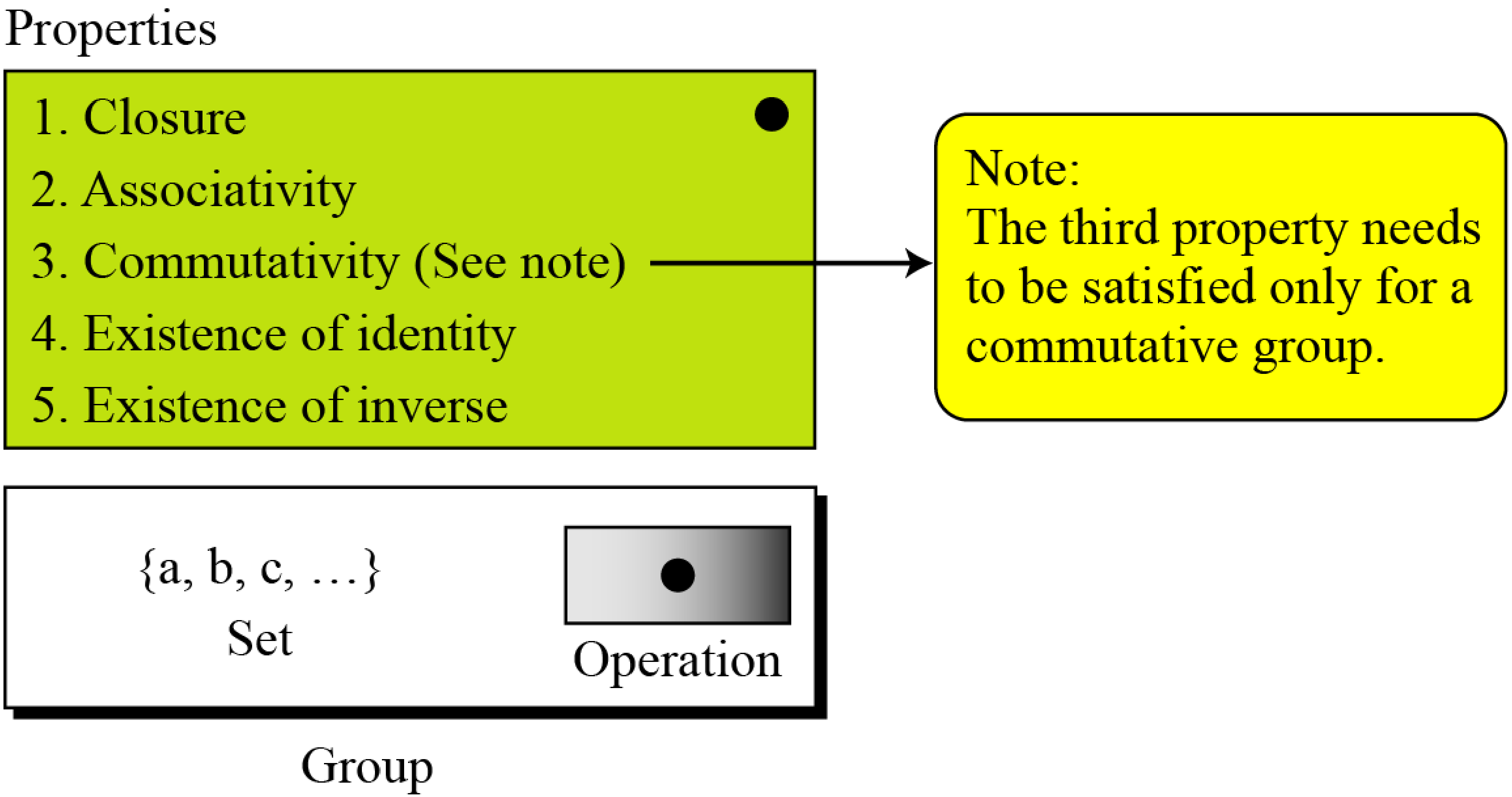
❑ Closure:

❑ Associativity:

❑ Commutativity:

❑ Existence of identity:

❑ Existence of inverse:



Properties

1. Closure ●
2. Associativity
3. Commutativity (See note)
4. Existence of identity
5. Existence of inverse

Note:
The third property needs to be satisfied only for a commutative group.

{a, b, c, …}

Set

●

Operation

Group

Cyclic subgroup

If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

$$\boxed{a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

Cyclic group

A cyclic group is a group that is its own cyclic subgroup.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

Examples: Three cyclic subgroups can be made from the group G = <Z10∗, ×>. G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are H1 = <{1}, ×>, H2 = <{1, 9}, ×>, and H3 = G.

a. The group G = <Z_6, +> is a cyclic group with two generators, *g* = 1 and *g* = 5.

b. b. The group G = <Z_{10}∗, ×> is a cyclic group with two generators, *g* = 3 and *g* = 7

Lagrange’s Theorem

Assume that G is a group, and H is a subgroup of G. If the order of G and H are |G| and |H|, respectively, then, based on this theorem, |H| divides |G|.

Order of an Element

The order of an element is the order of the cyclic group it generates.

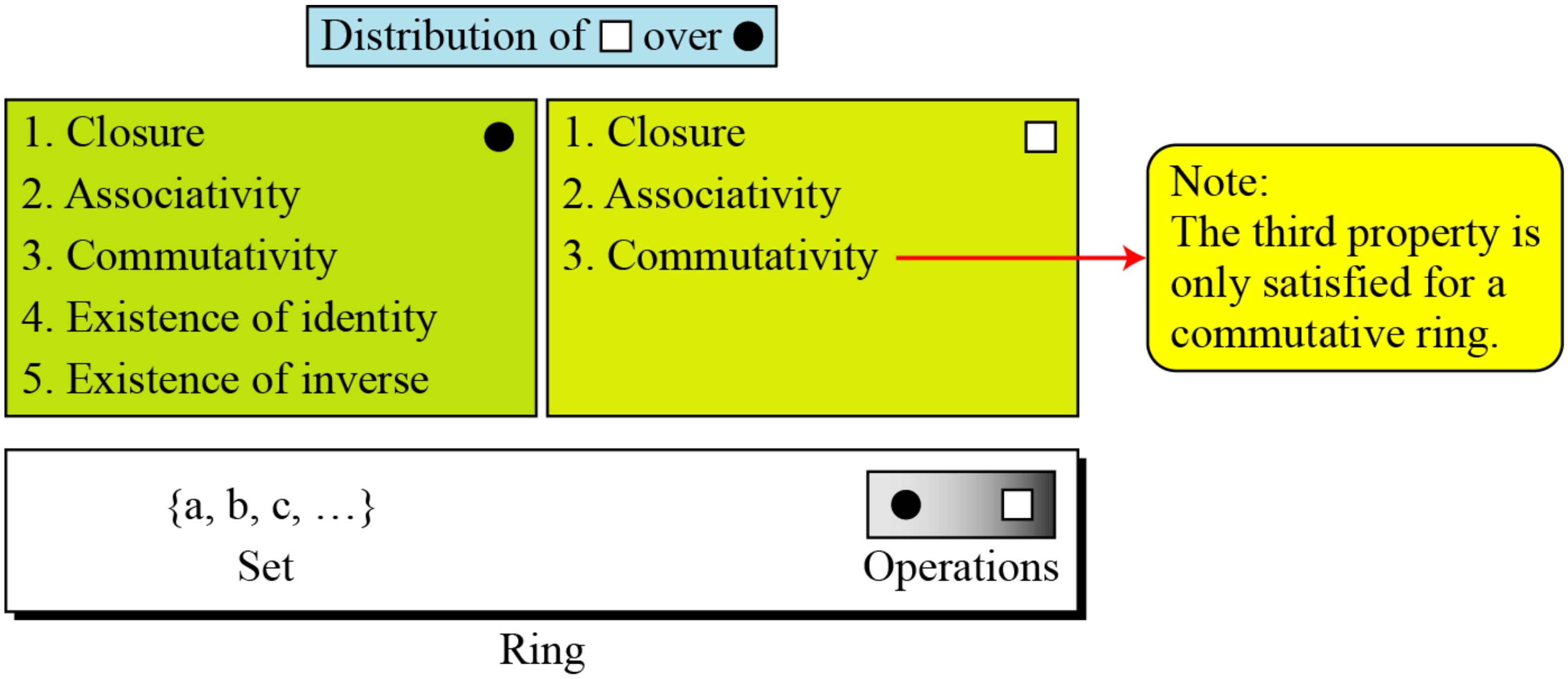
Examples:

- a. In the group G = <Z_6, +>, the orders of the elements are:
  ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.

- b. In the group G = <Z_{10}*, ×>, the orders of the elements are:
  ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

Ring

A ring, R = <{…}, •, >, is an algebraic structure with two operations.



Distribution of □ over ●

1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

1. Closure □
2. Associativity
3. Commutativity

Note:
The third property is only satisfied for a commutative ring.

{a, b, c, …}
Set

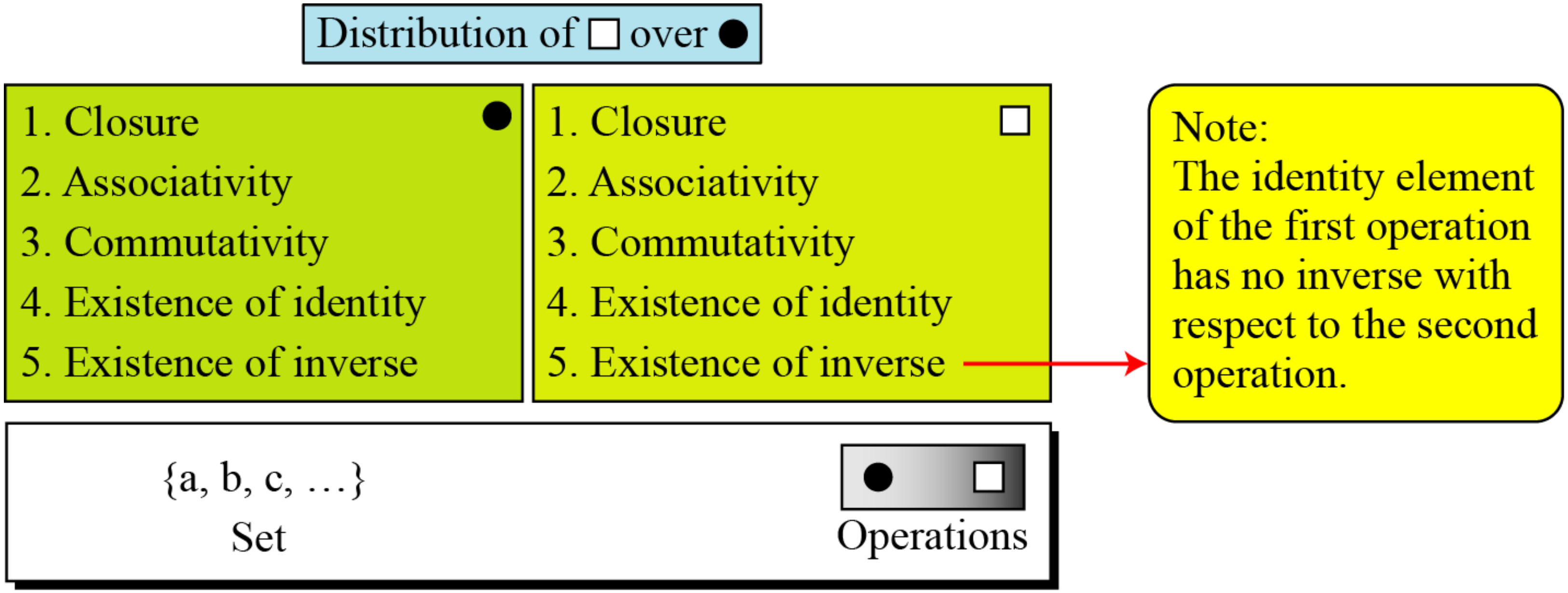
● □
Operations

Ring

Example: The set Z with two operations, addition and multiplication, is a commutative ring. We show it by R = <Z, +, ×>. Addition satisfies all of the five properties; multiplication satisfies only three properties.

Field

A field, denoted by F = <{…}, •, > is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.



Distribution of □ over ●

1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

1. Closure □
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

Note:
The identity element of the first operation has no inverse with respect to the second operation.

{a, b, c, …}
Set

● □
Operations

Field

Permutation Groups

A *permutation* of a set A is a function from A to A that is both one to one and onto.

Array Notation:

- Let A = {1, 2, 3, 4}
- Here are two permutations of A:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \qquad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

$$\alpha(2) = 3 \qquad \beta(4) = 3$$

$$\alpha(4) = 4 \qquad \beta(1) = 2$$

$$\beta\alpha(2) = \beta(3) = 4$$