HANU
HANOI UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Fall, 2024

DISCRETE MATHEMATIC LEC-04:

Fundamental Algebra
Groups, Rings, Fields

Lecture 4

- Sets, Operations
- Functions
- Groups, Rings and Fields

Sets

A collection of elements.

Examples:

- A set with all elements $A = \{a, b, c\}$
- A set with description of property $A = \{x : x > 3\}$
- The empty set, a set has no elements: $\emptyset$
- Set of integers: $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$
- Closed intervals: $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- Open intervals: $(a, b) = \{x \in \mathbb{R} : a < x < b\}$

Subsets

A subset (A) of a set (B) if every element of A is an element of B.

Examples:

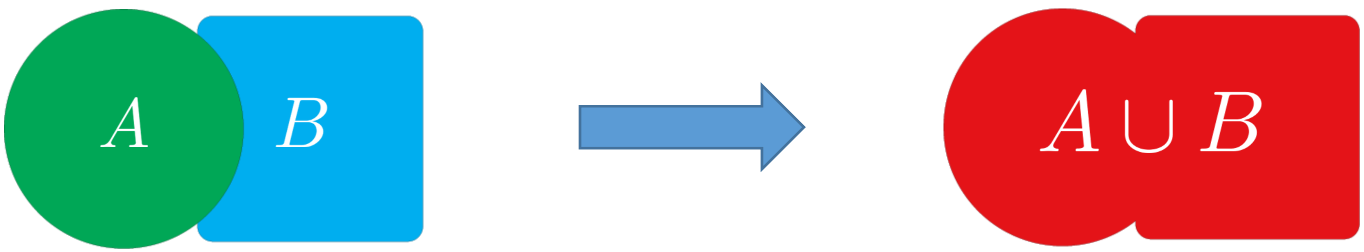
- Set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$
- Set of integers $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$

$\mathbb{N} \subset \mathbb{Z}$

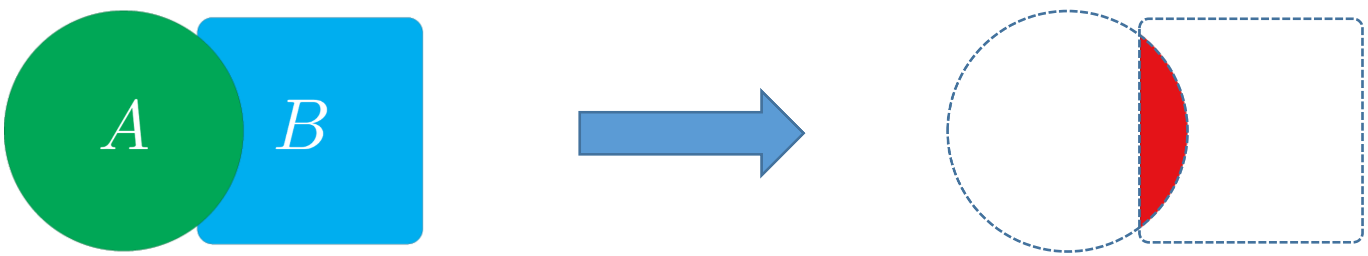
Set operations

<u>Examples:</u>

- Union: $A \cup B = \{x | \ x \in A \text{ or } x \in B\}$



- Intersection: $A \cap B = \{x | \ x \in A \text{ and } x \in B\}$

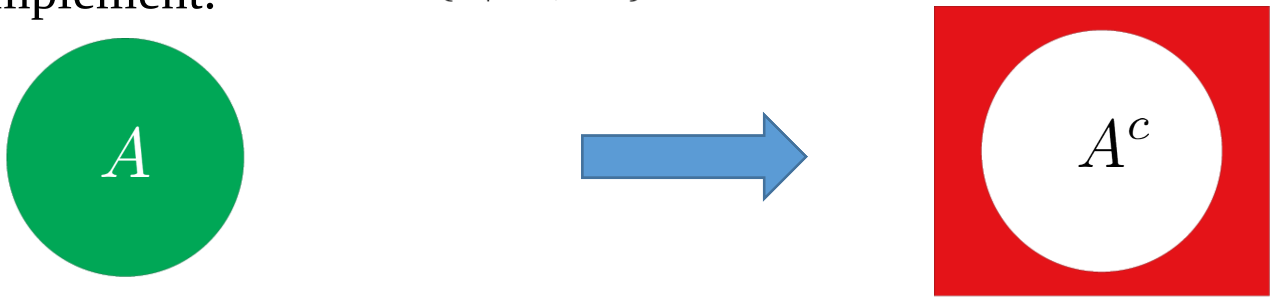


$A \cap B$

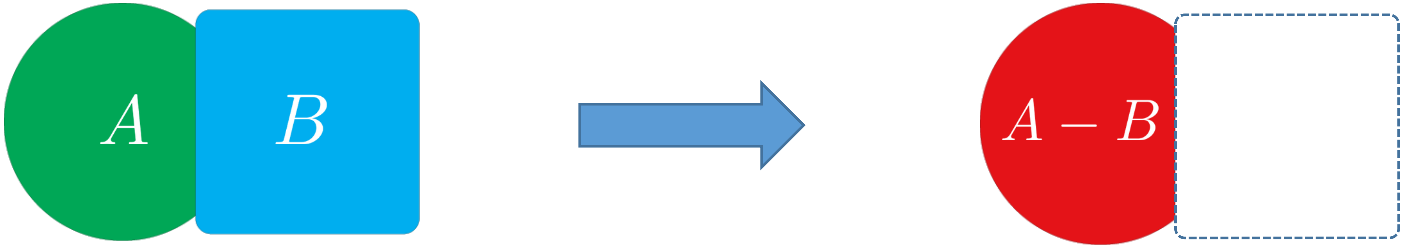
Set operations (cont'd)

<u>Examples:</u>

- Complement: A^c or $\bar{A} = \{x|\ x \notin A\}$



- Difference: $A - B$ or $A \backslash B = \{x|\ x \in A \text{ but } x \notin B\}$



Set Operations (cont'd)

<u>Laws that hold for sets:</u>

- Commutative: $A \cup B = B \cup A, A \cap B = B \cap A$
- Associative: $(A \cup B) \cup C = A \cup (B \cup C),$
  $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributive: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Idempotent: $A \cap A = A, A \cup A = A$
- Absorption: $A \cap (A \cup B) = A \cup (A \cap B) = A$
- Domination: $A \cup U = U, A \cap \emptyset = \emptyset$
- Identity: $A \cup \emptyset = \emptyset \cup A = A$

Example 1

Let A be the set of students who live within one mile of school and let B be the set of students who walk to classes. Describe the students in each of these sets.

1) $A \cap B$

the set of students who live within one mile of school and walk to class (only students who do both of these things are in the intersection)

2) $A \cup B$

the set of students who either live within one mile of school or walk to class (or, it goes without saying, both)

3) $A - B$

the set of students who live within one mile of school but do not walk to class

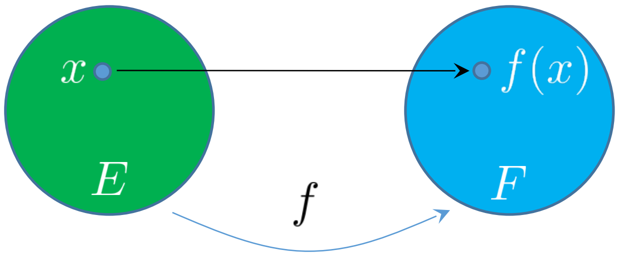
4) $B - A$

the set of students who live more than a mile from school but nevertheless walk to class

Functions

Let E and F be sets. Each element $x \in E$, *let there be associated a unique element* $f(x) \in F$, *then* f *is called a function from E into F.*

$$f : E \mapsto F$$



$f(x) \in F$ *: is called an image of* x.

Terms: mapping, operator, transformation are synonyms for the term function.

Injection, Surjection, Bijection

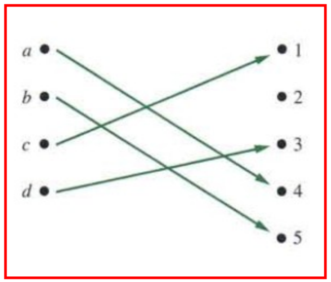
Let $f: A \mapsto B$, where A, B are sets.

Injection: Function f is called an injective mapping or injection or one-to-one-maping, if it maps different elements of set A to different elements of the set B.

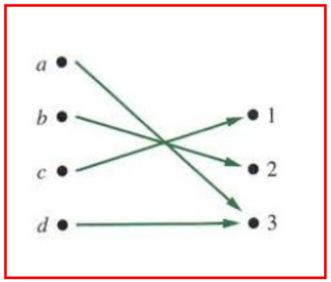
Surjection: Function f is called an surjective mapping or surjection or an onto maping, if for every element $x \in B$ there exits at least one element of A that is mapped to x.

Bijection: A mapping is called bijective mapping or bijection or a one-to-one correspondence if it is both surjective and injective.

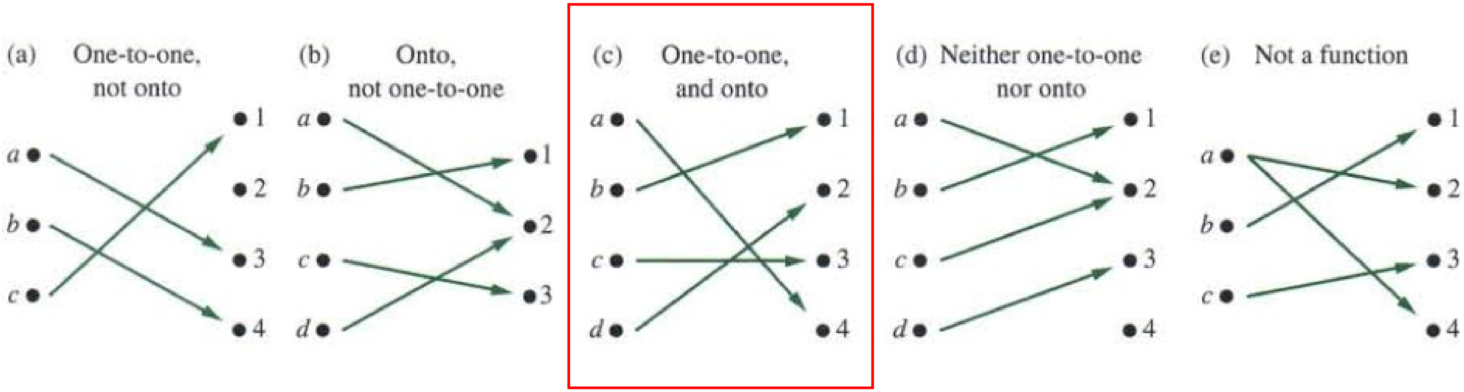
Injection, Surjection, Bijection



Injection
one-to-one-maping



Surjection
onto-maping



Bijection

Example 2

Why is f not a function from $\mathbb{R}$ to $\mathbb{R}$ if

1. $f(x) = 1/x$
2. $\sqrt{x}$
3. $f(x) = \pm\sqrt{(x^2+1)}$

1) The expression $1/x$ is meaningless for $x = 0$, which is one of the elements in the domain; thus the "rule" is no rule at all. In other words, $f(0)$ is not defined.

2) Things like $\sqrt{-3}$ are undefined (or, at best, are complex numbers).

3) The "rule" for f is ambiguous. We must have $f(x)$ defined uniquely, but here there are two values associated with every x, the positive square root and the negative square root of $x^2 + 1$.

Groups

Definition: Let (G, $\bullet$) be a nonempty set with a operation $\bullet$ defined on it: $a, b \mapsto a \cdot b$. Let the following axioms are satisfied:

- Closure: $\forall a, b \in G$, the element $a \cdot b$ is uniquely defined element of G.
- Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$
- Identity element: There exits an identity elements $I_G \in G$ such that
$$a \cdot I_G = I_G \cdot a = a \quad \forall a \in G$$
- Inverse element: for each $a \in G$ there exits an inverse element (denoted by $a^{-1} \in G$), such that $a \cdot a^{-1} = a^{-1} \cdot a = I_G$

We call G a group. Commutative: Abelian group

Groups (cont'd)

Definition: (Cyclic group) Let G be a group, and let a be any element of G. The set

$$\langle a \rangle = \{x \in G | x = a^n \text{ for some } n \in \mathbb{Z}\}$$

is called the cyclic subgroup generated by a. The group G is called a cyclic group if there exits an element $a \in G$ such that $G = \langle a \rangle$. The a is called a generator of G.

a^0 : Identity element

a^{-n} : Inverse element

Groups - Example

An example of group, G = (S, O, I) where S is set of integers O is the operation of addition, the inverse operation is subtraction I is the identity element zero (0).

Another example group, G = (S, O, I) where S is set of real numbers excluding zero O is the operation of multiplication, the inverse operation is division I is the identity element one (1).

The operation does not have to be addition or multiplication.

The set does not have to be numeric

Rings

Definition: (Ring) Let R be a set, with two operations: addition $(a, b \mapsto a+b)$ and multiplication $(a, b \mapsto a \cdot b)$ are defined where $\forall a, b \in R$. If the following holds, R is called a ring

a. "**Closure**": if $a, b \in R$, then the sum $(a+b)$ and the product $(a \cdot b)$ are uniquely defined and belong to R.

b. "**Associative laws**": We have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $(a+b)+c = a+(b+c) \quad \forall a, b, c \in R$.

c. "**Commutative laws**": We have $a+b = b+a$ and $a \cdot b = b \cdot a \quad \forall a, b \in R$.

d. "**Distributive laws**": We have $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$.

e. "**Additive Identity**": There exits an **additive identity element**, denoted by 0, such that $\forall a \in R,\ a+0 = a$ and $0+a = a$.

f. "**Additive Inverses**": for each $a \in R$, the equations $a+x = 0$ and $x+a = 0$ have a solution $x = -a$ called the **additive inverse** of a.

Rings - Example

A example ring, $R = (S, O_1, O_2, I)$

- S is set of real numbers.
- O_1 is the operation of addition, the inverse operation is subtraction.
- O_2 is the operation of multiplication.
- I is the identity element zero (0).

Fields

Definition: A ring R is called a **field**, if the multiplication is invertible for all $a \neq 0$. In other word, $\exists b \in R, b = a^{-1} \ \forall a \neq 0$, such that $a \cdot b = 1$.

Any fileld is ring.

Fields - Example

An example of field, F = (S, O_1, O_2, I_1, I_2)

- S is set of real number.
- O_1 is the operation of addition, the inverse operation is subtraction.
- O_2 is the operation of multiplication.
- I_1 is the identity element zero (0).
- I_2 is the identity element one (1).

More Examples

1. Does the following set A_{3x4} (set of all 3x4 matrices) and the operation • (matrix multiplication) form a group?
2. Prove that the set A_{3x3} (set of all 3x3 matrices) and the operation • (matrix addition) form a commutative (or Abelian) group.

Finite/Galois Fields

An example of field, $F = (S, O_1, O_2, I_1, I_2)$

- S is set of real number.
- O_1 is the operation of addition, the inverse operation is subtraction.
- O_2 is the operation of multiplication.
- I_1 is the identity element zero (0).
- I_2 is the identity element one (1).

REVIEW

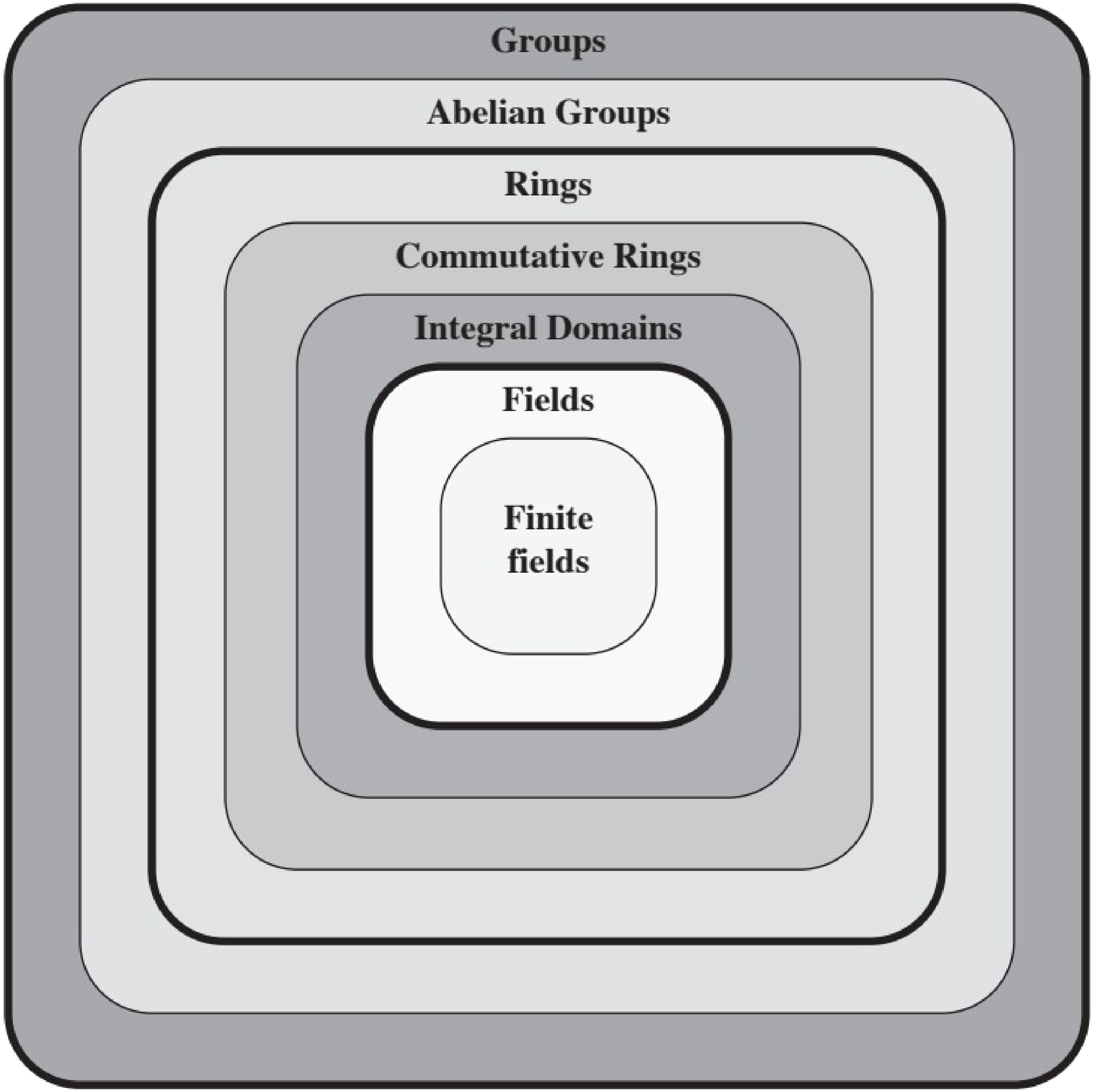


Figure 5.1 Groups, Rings, and Fields

Groups

- A set of elements with a binary operation denoted by □ that associates to each ordered pair (a,b) of elements in G an element (a □ b) in G , such that the following axioms are obeyed:
  - (A1) Closure:
    - If a and b belong to G, then a □ b is also in G
  - (A2) Associative:
    - a □ $(b$ □ $c)$ = $(a$ □ $b)$ □ c for all a, b, c in G
  - (A3) Identity element:
    - There is an element e in G such that a □ e = e □ a = a for all a in G
  - (A4) Inverse element:
    - For each a in G, there is an element a^{-1} in G such that a□a^{-1} = a^{-1} □ a = e

Abelian

  - (A5) Commutative:
    - a □ b = b □ a for all a, b in G

Cyclic Groups

- Exponentiation is defined within a group as a repeated application of the group operator, so that $a^3 = a \cdot a \cdot a$
- We define $a^0 = e$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group
- A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element a € G
- The element a is said to **generate** the group G or to be a **generator** of G
- A cyclic group is always abelian and may be finite or infinite

Rings

- A **ring** R , sometimes denoted by {R , + , * }, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a , b , c in R the following axioms are obeyed:

(A1–A5)

R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$

(M1) Closure under multiplication:

If a and b belong to R , then ab is also in R

(M2) Associativity of multiplication:

$a(bc) = (ab)c$ for all a , b , c in R

(M3) Distributive laws:

$a(b + c) = ab + ac$ for all a , b , c in R

$(a + b)c = ac + bc$ for all a , b , c in R

- In essence, a ring is a set in which we can do addition, subtraction $[a - b = a + (-b)]$, and multiplication without leaving the set

Rings contd.

- A ring is said to be commutative if it satisfies the following additional condition:

(M4) Commutativity of multiplication:

$ab = ba$ for all a, b in R

- An *integral domain* is a commutative ring that obeys the following axioms.

(M5) Multiplicative identity:

There is an element 1 in R such that $a1 = 1a = a$ for all a in R

(M6) No zero divisors:

If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$

Fields

- A **field** *F* , sometimes denoted by {F, +,* }, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all *a*, *b*, *c* in *F* the following axioms are obeyed:

  (A1–M6)

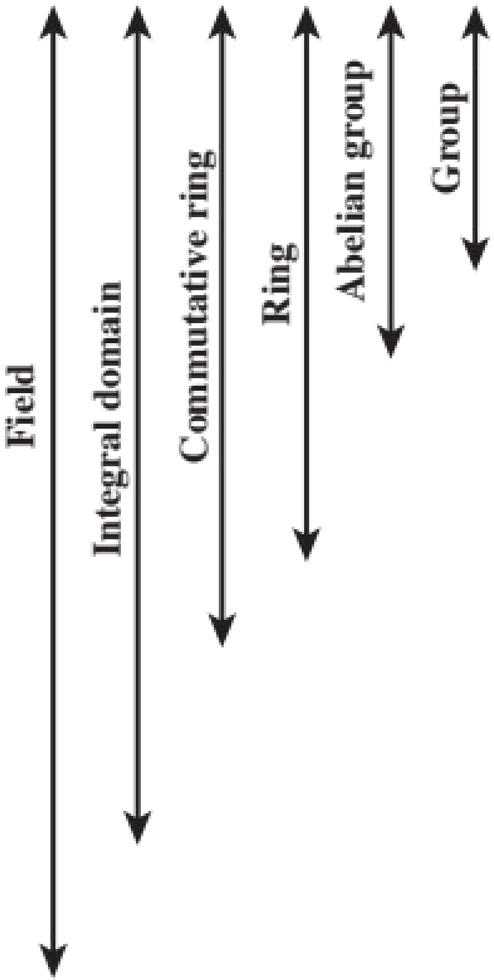
  F is an integral domain; that is, *F* satisfies axioms A1 through A5 and M1 through M6

  (M7) Multiplicative inverse:

  For each *a* in *F*, except 0, there is an element a^{-1} in *F* such that $aa^{-1} = (a^{-1})a = 1$

- In essence, a field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the foll

Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse.



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 5.2 Properties of Groups, Rings, and Fields

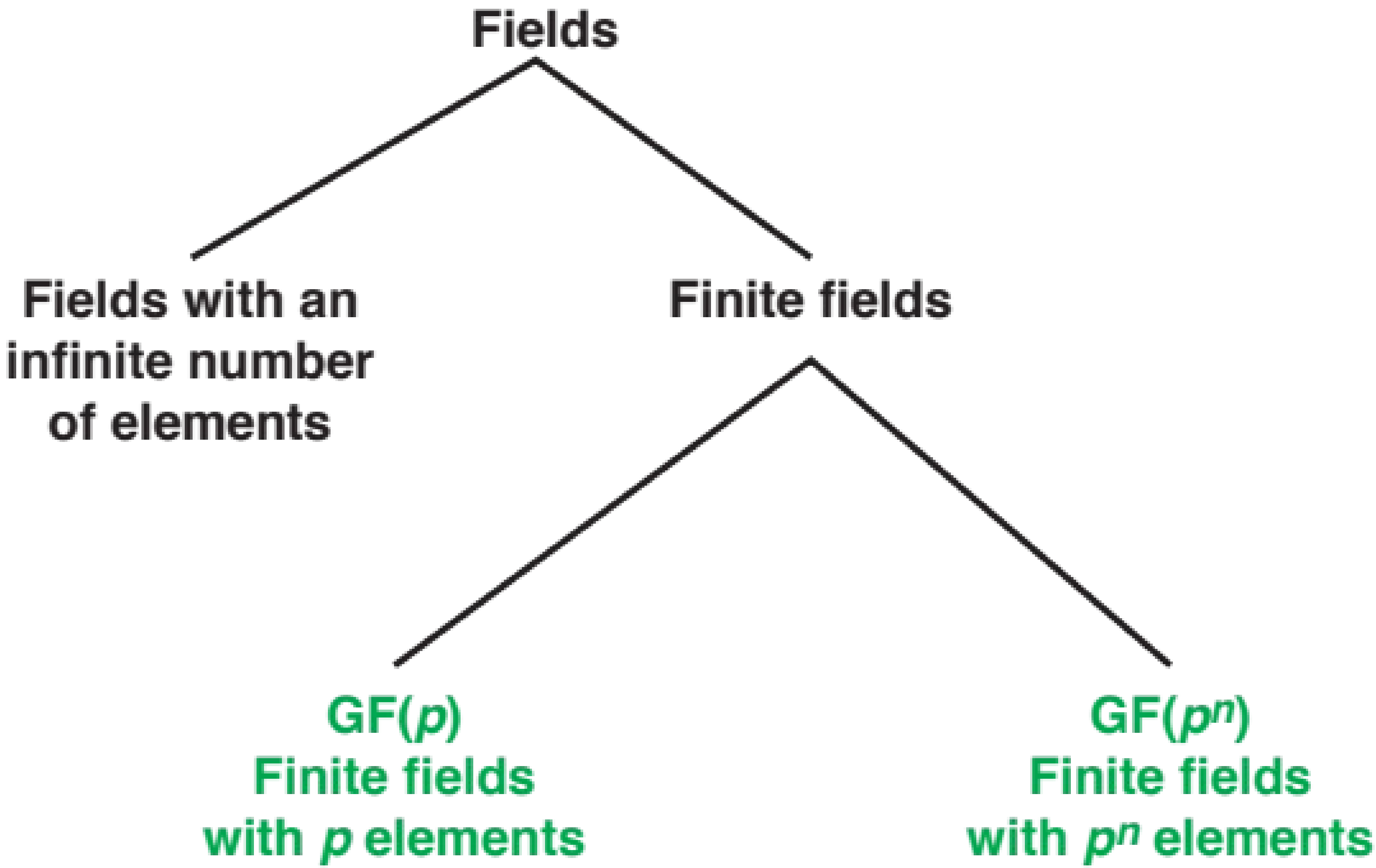


Figure 5.3 Types of Fields

Finite Fields of the Form GF(p)

- Finite fields play a crucial role in many cryptographic algorithms
- It can be shown that the order of a finite field must be a power of a prime p^n, where n is a positive integer
  - The finite field of order p^n is generally written GF(p^n)
  - GF stands for Galois field, in honor of the mathematician who first studied finite fields

Table 5.1(a)

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Table 5.1(b)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Table 5.1(c)

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

Table 5.1(d)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(d) Addition modulo 7

Table 5.1(e)

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(e) Multiplication modulo 7

Table 5.1(f)

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(f) Additive and multiplicative inverses modulo 7

In this section, we have shown how to construct a finite field of order p, where p is prime.

GF(p) is defined with the following properties:

- 1. GF(p) consists of p elements
- 2. The binary operations + and * are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse
- We have shown that the elements of GF(p) are the integers {0, 1, . . . , p – 1} and that the arithmetic operations are addition and multiplication mod p