DEFN A **binary operation** \( * \) on a set \( G \) is a rule that for each \( a \in G, b \in G \) assigns \( c = a * b \), such that \( c \in G \).

DEFN A **group** consists of a set \( G \) and a binary operation \( * \) with the following properties:

1. **Associativity** \( (a * b) * c = a * (b * c) \) for \( a, b, c \in G \)
2. **Existence of Identity** There exists \( e \in G \) such that \( a * e = e * a = a \), for all \( a \in G \)
3. **Existence of Unique Inverses** For each \( a \in G \), there exists a unique element \( a^{-1} \in G \) such that \( a * a^{-1} = a^{-1} * a = e \)

DEFN A group is said to be **commutative** or **abelian** if it also satisfies:

4. **Commutativity**: For all \( a, b \in G \), \( a * b = b * a \)

- If a group is commutative, then the group operation is often represented as “+”
- Examples of groups:
  - The **set of integers** forms a commutative group under **addition**.
  - The **set of integers** does **not** form a group under **multiplication**. Why?
  - The **set of rational numbers excluding zero** forms a group under **multiplication**.
  - The **set of \((n \times n)\) matrices with real elements** forms a commutative group under matrix addition.

DEFN The **order**, or **cardinality** of a group is the number of elements in the group.

DEFN If the order or a group is finite, the group is a **finite group**. Otherwise, it is an **infinite group**.

- The previous examples are **infinite groups**.
• For the construction of error-control codes, we are primarily concerned with finite groups.
• Construction of finite groups using modulo arithmetic on the integers:
  – The result of **addition modulo** \( m \) of \( a, b \in G \) is the remainder, \( c \), of \( a + b \) divided by \( m \), where \( 0 \leq c \leq m - 1 \):
    \[
    a + b = k \cdot m + c,
    \]
    where \( k \) is the largest integer such that
    \( k \cdot m < (a + b) \)
  – Modulo addition can be expressed in several ways. We will start with a more-descriptive form than in the text:
    \[
    a + b \equiv c \mod m
    \]
  – Examples - on board

**Construction of Groups Using Modulo Addition**

– Define \( G \) by \( G = \{0, 1, 2, \ldots, m - 1\} \)
– Define \( c = a \oplus b \) by \( a + b \equiv c \mod m \)
– Then \( (G, \oplus) \) is a group:
  * \( a \oplus b \) is an integer between 0 and \( m - 1 \), so \( G \) is **closed under** \( \oplus \)
  * \( \oplus \) is **associative** – see textbook
  * The identity element under \( \oplus \) is zero
    \[
    a \oplus 0 = a,
    a \oplus b = a \Rightarrow b = k \cdot m,
    \]
    but \( b = k \cdot m \Rightarrow b = 0 \)
    (The identity is unique)
  * For an element \( a \) in \( G \), \( m - a \) is also in \( G \).
    Let \( c = a \oplus m - a \). Then
    \[
    a + m - a \equiv c \mod m
    \]
    \[
    m \equiv c \mod m
    \]
    \[
    \Rightarrow m = k \cdot m + c
    \]
    \[
    \Rightarrow c = 0
    \]
    (Inverses are in \( G \).
  * This defines an **additive group** over the integers mod \( m \).
  * Example – on board
• **Construction of Groups Using Modulo Multiplication**
  
  - Suppose we select a prime number \( p \), and let \( G = \{ 1, 2, \ldots, p - 1 \} \).
  - Define \( \Box \) by \( c = a \Box b \) if \( a \cdot b \equiv c \mod p \).
  - **Claim**: \((G, \Box)\) is a group of order \( p - 1 \)
    * **Associativity**: see proof on board
    * **Identity**: clearly \( a \Box 1 = a \)
    * **Inverses**:
      Let \( i \in G \) be an element for which we want to find an inverse
      By Euclid’s Theorem, \( \exists \ a, b \) such that
      \[ a \cdot i + b \cdot p = 1 \]
      if \( a, p \) are relatively prime (guaranteed since \( p \) is prime and \( a < p \)).
      Then
      \[ a \cdot i = -b \cdot p + 1 \]
      \[ \Rightarrow a \cdot i \equiv 1 \mod p \]
      If \( a \in G \), then \( i^{-1} = a \).
      If \( a \notin G \), divide \( a \) by \( p \),
      \[ a = q \cdot p + r, \ \text{where} \ r \in G \]
      Then
      \[ (q \cdot p + r) i = -b \cdot p + 1 \]
      \[ r \cdot i = -(qi + b) \cdot p + 1, \]
      so \( r \in G \) and \( r \cdot i \equiv 1 \mod p \), \( \Rightarrow i^{-1} = r \).

• **Properties of Groups**
  
  - **Theorem 2.1** The identity element is unique.
  (Proof omitted)
  - **Theorem 2.2** The inverse of a group is unique.
  Suppose \( a \in G \) has 2 inverses \( a' \) and \( a'' \)
  Then
  \[ a' = a' \ast e \]
  \[ = a' \ast (a \ast a'') \]
  \[ = (a' \ast a) \ast a'' \]
  \[ = e \ast a'' = a'' \]
  
  Thus, \( a' = a'' \), and the inverse is unique.
**Subgroups:** If $H$ is a nonempty subset of $G$ and $H$ is closed under $*$ and satisfies all the conditions of a group, then $H$ is a *subgroup* of $G$.

**Rings**

**DEFN** A *ring* is a collection of elements $R$ with two binary operations, usually denoted “$+$” and “$\cdot$” with the following properties;

1. $(R, +)$ is a commutative group. The additive identity is labeled “0”.
2. $\cdot$ is Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $\cdot$ Distributes over $+$. 
   \[ a \cdot (b + c) = (a \cdot b) + (a \cdot c). \]

**DEFN** A ring is a *commutative ring* if $\cdot$ is commutative: $a \cdot b = b \cdot a$

**DEFN** A ring is a *ring with identity* if $\cdot$ has an identity, which is labeled “1”.