# Chapter 7.1A    part 1

# Group Theory

## Section 7.1 A

Recall: Ring is a set with two operations

**Def** Group is a non-empty set $G$ equipped with a binary operation $*$ that satisfies

1. For $a \in G$, $b \in G$, we have $a * b \in G$ } binary operation
2. $a * (b * c) = (a * b) * c$ } associativity

   we can write $a * b * c$ without parenthesis
3. There is $e \in G$ (identity element) such that $e * a = a * e = a$ for every $a \in G$ } analog of 0 for addition, 1 for multiplication in rings
4. For each $a \in G$, there is $d \in G$ such that $a * d = d * a = e$ } inverse of $a$. Notation: $a^{-1}$

---

5. A group is called abelian if we have $a * b = b * a$ for every $a, b \in G$ } non-abelian otherwise

Finite group $G$ means the set $G$ is finite } otherwise - infinite group
(a group of finite order) infinite order

The order of a group $G$ - the amount of elements in the set $G$ } Notation: $|G|$

Examples of groups

$\{e\}$ - the set of one element | Finite abelian group of order one

$e * e = e$

$\mathbb{Z}$ - set of integers - group with respect to addition - infinite abelian group

Th 7.1 If $R$ is a ring, then $R$ is an abelian group with respect to addition. $0_R$ - the identity

With the exception of zero ring $\{0_R\}$,
a ring is not a group with respect to the multiplication.
The obstacle is $0_R \in R$ which is never invertible

Th 7.2 If $R$ is a field, then $R^* = R \setminus \{0_R\}$ is an abelian group with respect to multiplication
(iff statement) $e = 1_R$ - the identity

Although $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ is not a group w.r.t. <u>multiplication</u>,

$\{1, -1\}$ is a group ——— " ———

finite group of order 2.

Th 7.3 For a ring $R$ with identity $1_R \in R$, the <u>set of units of $R$</u> is a group with respect to multiplication

In this way $\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Z}_p^*$ - abelian groups

p - prime

---

Examples: $\mathbb{Q}^{**}$ - positive rational numbers with respect to multiplication | $e = 1$

$\mathbb{R}^{**}$ —— real ——— " ——

Example 11 $\{1, -1, i, -i\} \subset \mathbb{C}$ is a group of order 4 with respect to multiplication (as complex numbers)