Lecture 1: Rings and Subrings

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Rings

Definition

Let R be a nonempty set and the two binary operations $+$(addition) and .(multiplication) defined on R. $(R, +, .)$ is called a ring if the following conditions are satisfied:

R_1) $(R, +)$ is an abelian group.

R_2) Multiplication is associative.

R_3) The left and right distributive laws holds; that is, for all $a, b, c \in R$

$$\begin{aligned} a.(b+c) &= (a.b)+(a.c) \\ (a+b).c &= (a.c)+(b.c). \end{aligned}$$

For simplicity we denote

$$\begin{aligned} R &:= (R, +, .) \\ ab &:= a.b \\ a-b &:= a+(-b). \end{aligned}$$

Some remarks:

- The additive identity element (zero element) of the ring R is 0_R. The additive inverse of an element a is $-a$.
- A ring R is called a *commutative ring* if the multiplication is commutative.
- A ring R is called a *ring with unity(identity)* if it has a multiplicative identity. (The multiplicative identity element is denoted by 1_R). We should note that if a ring has a multiplicative identity element, it is unique.
- Let R be a ring with unity 1_R. An element $u \in R$ is called a *unit* (invertible element) if $\exists v \in R$ such that $uv = vu = 1$.(The multiplicative inverse of an element a (if exists) is denoted by a^{-1})
- Let the set of all units of R is $U(R) := \left\{u \in R \mid u^{-1} \in R\right\}$. Then
  (i) $\varnothing \neq U(R)$
  (ii) $0_R \notin U(R)$
  (iii) $(U(R), .)$ is a group.

Rings

Examples:

1. $(\mathbb{Z},+,.)$ is a commutative ring with unity 1.
2. $(\mathbb{R},+,.)\,,(\mathbb{Q},+,.)\,,(\mathbb{C},+,.)$ are commutative rings with unity.
3. $(\mathbb{Z}_n,+_n,._n)$ is a commutative ring with unity $\overline{1}$.
4. $(2\mathbb{Z},+,.)$ is a commutative ring without unity.
5. $(M_2(\mathbb{Z}),\oplus,\odot)$ is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.(The operations $\oplus,\odot$ are matrix addition and matrix product, respectively).
6. $(M_2(2\mathbb{Z}),\oplus,\odot)$ is a noncommutative ring without unity.
7. The zero ring $(\{0_R\},+,.)$ is the only ring in which 0_R could act as additive identity and multiplicative identity.
8. $\mathbb{Z}[i] := \{a+ib \mid a,b\in\mathbb{Z}\}$ is a ring with the usual operations on complex numbers. ($\mathbb{Z}[i]$ is called the ring of Gaussian integers)

Definition

Let R and S be any two rings. $R \times S = \{(r, s) \mid r \in R, s \in S\}$ is a ring with the operations $+$ and $.$ that are defined componentwise. The ring $(R \times S, +, .)$ is called the **direct product** of rings R and S.

Example: $(\mathbb{Z} \times \mathbb{Z}, +, .)$ is a commutative ring with unity $(1, 1)$.

Definition

$M(R) := \{a \in R \mid ax = xa, \text{for all } x \in R\}$ is called the **center** of the ring R.

$M(R) = R \Leftrightarrow R$ is a commutative ring.

Definition

Let R be a ring. An element $a \in R$ is called an **idempotent** element if $a^2 = a$. A ring R is called a **Boolean ring** if every element of R is idempotent.

Theorem

Every Boolean ring is commutative.

Examples:

1. $\mathbb{Z}$ is not a Boolean ring. The only idempotents are 0 and 1.
2. $\mathbb{Z}_2$ is a Boolean ring.
3. $\mathbb{Z} \times \mathbb{Z}$ is not a Boolean ring. The only idempotents are $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$.

Definition

Let R be a ring. An element $a \in R$ is called a **nilpotent** element if $a^n = 0_R$ for some positive integer n.

If a nonzero element $a \in R$ is idempotent, then it is not a nilpotent.

Elementary properties of rings

Let R be a ring. For $n \in \mathbb{Z}, a \in R$,

$$n.a = \begin{cases} \underbrace{a + a + \cdots + a}_{n}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{|n|}, & n < 0. \end{cases}$$

Theorem

Let R be a ring. For $a, b, c \in R$, we have

1) $a0_R = 0_R a = 0_R$,
2) $a(-b) = (-a)b = -(ab)$,
3) $(-a)(-b) = ab$,
4) $a(b - c) = ab - ac$.

Remark: Let $\{0_R\} \neq R$ be a ring with unity. Then the elements 0_R and 1_R are distinct. Hence, in a ring $\{0_R\} \neq R$ with unity, there exists at least two elements.

Subrings

Definition

Let $(R,+,.)$ be a ring and $\emptyset \neq S \subseteq R$. $(S,+,.)$ is called a subring of R (denoted by $S \leq R$) if S is a ring with the operations of R.

Theorem

Let $(R,+,.)$ be a ring and $\emptyset \neq S \subseteq R$.

$$S \leq R \Leftrightarrow \begin{array}{l} (i)\ \forall a,b \in S,\ \ a-b \in S \\ (ii)\ \forall a,b \in S,\ \ ab \in S \end{array}$$

Examples:

1. $\{0_R\} \leq R,\ R \leq R$
2. $2\mathbb{Z} \leq \mathbb{Z}$
3. $M_2(2\mathbb{Z}) \leq M_2(\mathbb{Z})$
4. $\mathbb{Z}[i] \leq \mathbb{C}$
5. $\{\overline{0},\overline{2},\overline{4}\} \leq \mathbb{Z}_6$
6. $M(R) < R$

Remarks:

- If R is a commutative ring, then every subring of R is commutative.
- If R is ring with unity, a subring of R need not have unity (or need not have same unity).
  In Example 2, $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ without unity.
  In Example 5, the unity of subring $\{\overline{0}, \overline{2}, \overline{4}\}$ is $\overline{4}$, although the unity of $\mathbb{Z}_6$ is $\overline{1}$.