(Chapter 16) Rings

(§ 16.1) Rings

Def.: A non-empty set R is a ring if it has two binary operations, addition $a+b$ and multiplication ab s.t. for $\forall a, b, c \in R$ the following axioms are satisfied:

1) $a+b=b+a$ (commutativity of addition)
2) $(a+b)+c = a+(b+c)$ (associativity of addition)
3) $\exists$ an additive identity $0 \in R$, that is, $a+0=a \quad \forall a \in R$.
4) $\forall a \in R \ \exists -a \in R$ s.t. $a+(-a)=0$. (additive inverse)
5) $a(bc) = (ab)c$ (associativity of multiplication)
6) $a(b+c) = ab+ac$ & $(a+b)c = ac+bc$. (distributivity, relates addition & multiplication)

- Thus, a ring is an abelian group under addition (axioms 1)-4))
- Note: $ab \neq ba$ in general. If $ab=ba \ \forall a, b \in R$ then the ring R is called <u>commutative</u>.
- A ring does not have to have a multiplicative identity. If a ring R has an element 1 s.t. $1 \neq 0$ and $1a = a1 = a \ \forall a \in R \Rightarrow$ we say <u>R is with unity or identity</u>.
- A commutative ring R w/ identity is called an <u>integral domain</u> if, $\forall a, b \in R$, s.t. $ab=0 \Rightarrow a=0$ or $b=0$. (R has no zero divisors.)
- Note: an element $a \neq 0 \in R$ (ring) does not have to have $a^{-1} \in R$, s.t. $aa^{-1} = a^{-1}a = 1$. If $a \in R$ has such a^{-1}, then a is called a <u>unit</u>. R where any $a \neq 0$ is a unit, is called a <u>division ring</u>. (division ring, of course, has 1)
- <u>Field</u> is a commutative division ring.

Rings

Rings w/ identity (unity)
$\exists 1 \neq 0$ s.t. $a1 = 1a = a$ $\forall a \in R$

Commutative Rings
($ab = ba$, $\forall a, b \in R$)

Integral Domains
(no zero divisors:
$\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$)

Division Rings
($\forall a \in R, a \neq 0, \exists a^{-1} \in R$)
$aa^{-1} = a^{-1}a = 1$
unit

a is a zero divisor if $a \neq 0$ in R and $ab = 0$ for some $b \neq 0$.

Fields (= commutative division rings)
(are integral domains:

$\forall a, b$ s.t. $ab = 0$, let $a \neq 0$
$\Rightarrow a^{-1}ab = a^{-1}0 \Rightarrow b = 0$
if $b \neq 0 \Rightarrow a = 0$)

Examples of Rings:

① $\mathbb{Z}$ under ordinary addition & multiplication is a commutative ring w/ unity 1.
($ab = ba$)

The only units of $\mathbb{Z}$ are 1 and -1

(they are their own inverses: $1 \cdot 1 = 1$, $(-1)(-1) = 1$)

$\forall a \in \mathbb{Z}, a \neq \pm 1$: $\nexists a^{-1}$ s.t. $aa^{-1} = a^{-1}a = 1$ (e.g., $a = 2 \Rightarrow \nexists 2^{-1}$ ($\frac{1}{2} \notin \mathbb{Z}$))

Note: If $a, b \in \mathbb{Z}$ and $ab = 0$
$\Rightarrow a = 0$ or $b = 0$ in $\mathbb{Z}$. So, $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}$ is not a field:

$\nexists a^{-1}$ $\forall a \in \mathbb{Z}$.

2. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring w/ unity 1. Recall: $U(n) = \{x \in \mathbb{Z}_n, \gcd(x,n)=1\}$ is the group of units in $\mathbb{Z}_n$ (so the units of $\mathbb{Z}_n$ are all elements of $U(n)$). Note $\mathbb{Z}_n$ may fail to be an integral domain: consider, for example, $a=3$ and $b=4$ in $\mathbb{Z}_{12}$, $3 \cdot 4 \equiv 0 \pmod{12}$, but $a \neq 0, b \neq 0 \Rightarrow$ a product of two nonzero elements in $\mathbb{Z}_n$ may be equal to zero. ($\mathbb{Z}_p$ is a field if p is prime)

3. Other rings: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ under ordinary addition & multiplication. In fact, they are fields (commutative division rings: $ab = ba$, $\forall a \in F$, $\exists a^{-1} \in F$ s.t. $aa^{-1} = a^{-1}a = 1 \leftarrow$ mult. id.)
unit ← mult. inverse

4. $2\mathbb{Z}$ (the set of even integers) is a commutative ring (under addition / multiplication) without unity.

$2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$

$\nexists$ id s.t. $a \cdot id = id\, a = a \quad \forall a \in 2\mathbb{Z}$

5. The set of all continuous, real-valued functions on an interval $[a,b]$ ($C[a,b]$) forms a commutative ring w/ unity $f(x) \equiv 1$

$fg = gf$ $\quad (f+g)(x) = f(x) + g(x)$
$(fg)(x) = f(x) \cdot g(x)$

(Not an integral domain: $fg = 0$ w/ $f = \begin{cases} 0, & x \le 0 \\ x, & x > 0 \end{cases}$ $g = \begin{cases} x, & x \le 0 \\ 0, & x > 0 \end{cases}$ on $(-\infty, \infty)$)

6. $\mathbb{Z}[x]$ is the set of all polynomials in a variable x w/ integer coefficients forms a commutative ring under addition & multiplication, w/ unity $f(x) \equiv 1$.

(in fact, $\mathbb{Z}[x]$ is an integral domain, but not a field)

Why?

7. The set of 2×2 matrices w/ real entries form a (noncommutative) ring w/ unity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and AB can be 0 if $A \neq 0$, $B \neq 0$.
$AB \neq BA$
($\Rightarrow$ not an integral domain).

8. See (long) Example 16.7 in §16.1 : the ring of quaternions.

<u>Note:</u> <u>never</u> treat a ring R as a multiplicative group : if $a, b, c \in$ ring R $\not\Rightarrow$ if $ab = ac \Rightarrow b = c$ or if $a^2 = a \Rightarrow a = 1$ or $a = 0$.

<u>Proposition (16.8)</u>: <u>Properties of Rings.</u>

Let R be a ring, w/ $a, b \in R$. Then

(1) $a0 = 0a = 0$
(2) $a(-b) = (-a)b = -(ab)$
(3) $(-a)(-b) = ab$.

From here, $a(b-c) \overset{(2)}{=} ab - ac$; $(b-c)a \overset{(2)}{=} ba - ca$; $b + (-c)$
$\underbrace{(-1)a \underset{(2)}{=} -a \; ; \quad (-1)(-1) \underset{(3)}{=} 1}_{\text{if } R \text{ has a unity}}$

<u>Proof:</u> (1) $0 + a0 = a0 = a(0+0) = a0 + a0 \Rightarrow$
$0 + a0 = a0 + a0 \Rightarrow$ by cancellation, $0 = a0$.
Similarly, $0a = 0$.

(2) $ab + a(-b) = a(b-b) = a0 = 0 \Rightarrow$ adding $-(ab)$ to both sides of $ab + a(-b) = 0$, we get $a(-b) = -(ab)$. Similarly, $(-a)b = -(ab)$.

(3) $(-a)(-b) \underset{(2)}{=} -(a(-b)) = -(-ab) = ab$ $\square$

<u>Note:</u> If a ring has a unity, it is <u>unique</u>. If a ring element has a multiplicative inverse, it is <u>unique</u>.

- Groups have subgroups and rings have <u>subrings</u>

<u>Def:</u> A subset S of a ring R is a subring of R if S itself is a ring under the operations in R.

<u>Examples of Subrings:</u>

1. $\{0\}$ and R are subrings of R.
   (trivial subrings)

2. $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is a subring of $\mathbb{Z}$.

3. $\underbrace{S = \{0,2,4\}}_{\text{unity is } 4}$ is a subring of $\underbrace{\mathbb{Z}_6 = \{0,1,2,3,4,5\}}_{\text{unity is } 1}$.

   both comm. rings

   $\forall s \in S$, $4 \cdot s = s \cdot 4 = s$:
   $4 \cdot 0 = 0 \cdot 4 = 0$
   $4 \cdot 2 = 2 \cdot 4 = 2 \pmod 6$
   $4 \cdot 4 = 4 \pmod 6$

   $\forall a \in \mathbb{Z}_6$, $a \cdot 1 = 1 \cdot a = a$

4. Chain of subrings: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

5. The set of Gaussian integers $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

<u>Proposition (16.10)</u>: <u>Subring Test.</u> $\rightarrow$ <u>HW exer.</u>

Let R be a ring and $S \subset R$. Then S is a subring of R if and only if:

1) $S \neq \emptyset$; 2) $rs \in S$ $\forall r, s \in S$ (closure); 3) $r - s \in S$ $\forall r, s \in S$. (analog of rs^{-1})

Example:

Let $R = M_2(\mathbb{R})$ be the set of 2×2 matrices w/ entries in $\mathbb{R}$. R is a ring. Consider

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a,b,c \in \mathbb{R} \right\},$$ then T is a subring of R.

Why?

1) $T \neq \emptyset$ since $\underbrace{I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{unity in } R} \in T$

2,3) If $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ are in T

then $AB = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}$ is also in T and

$A - B = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix}$ is in T as well. $\square$