Rings

Definition A ring R is a set with two binary operations: addition $a+b$
and multiplication ab
satisfy the following conditions

1. $a+b=b+a$
2. $(a+b)+c=a+(b+c)$ $\forall a, b, c \in R$
3. $\exists$ an additive identity 0 : $a+0=a$ $\forall a$
4. $\exists$ an element $-a \in R$ s.t. $a+(-a)=0$ $\forall a$
5. $(ab)c=a(bc)$ $\forall a, b, c$
6. $a(b+c)=ab+ac$ $(b+c)a=ba+ca$

So a ring is an abelian group under addition, also have an associative multiplication that is left and right distributive over addition

- the multiplication need not be commutative, When it is, we say the ring is commutative
- A unity (or identity): a nonzero element that is an identity under multiplication.
- unit: a nonzero element of a commutative ring with identity that has a multiplicative inverse.

- In R, $a \mid b$ if $\exists c \in R$ s.t. $b = ac$
- $n \in \mathbb{Z}_{>0}$ $\quad na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$

Ex1 $(\mathbb{Z}, +, \cdot)$ commutative ring with identity
units: ± 1

Ex2 $(\mathbb{Z}_n, +, \cdot)$ commutative ring with identity
units: $U(n)$

Ex3 $(\mathbb{Z}[x], +, \cdot)$ commutative ring with identity

Ex4 $(M_2(\mathbb{Z}), +, \cdot)$ non-commutative ring with identity

Ex5 $(2\mathbb{Z} = \{\text{even integers}\}, +, \cdot)$ comm ring without identity

Ex6 $(\{\text{continuous fcns on } \mathbb{R}\}, +, \cdot)$
comm ring with identity $f(x) = 1$

Ex6' $(\{\text{continuous fcns on } \mathbb{R} \text{ whose graph pass through } \underline{(1,0)}\}, +, \cdot)$
comm ring without identity

$\boxed{\begin{array}{l} f(1)=0 \quad g(1)=0 \\ f+g, \ fg \end{array}}$

Ex7 $R_1, R_2, \cdots, R_n$ be rings. construct

$R_1 \oplus R_2 \oplus \cdots \oplus R_n$

$= \{(a_1, a_2, \cdots a_n) \mid a_i \in R_i\}$

endowed with componentwise addition and multiplication. This is called the <u>direct sum</u> of $R_1, R_2, \cdots, R_n$

<u>Properties of rings</u>

* 1) $a \cdot 0 = 0 \cdot a = 0 \quad \forall a$
2) $a(-b) = (-a)b = -(ab)$
3) $(-a)(-b) = ab$
4) $a(b-c) = ab - ac \quad (b-c)a = ba - ca$
5) $(-1)a = -a$
6) $(-1)(-1) = 1$

} if R has an identity 1

$$a \cdot (0+0) = a \cdot 0 + (a \cdot 0 - a \cdot 0) = a \cdot 0$$

$$a \cdot 0 - a \cdot 0 = 0$$

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

Pf: $1, 1' \Rightarrow 1 = 1 \cdot 1' = 1'$

$a \qquad ab = ba = 1$

$$ac = ca = 1$$
$$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b \quad \square$$

Warning: In general $ab = ac \not\Rightarrow b = c$
(cancelation rule does not hold in general for multiplication)

Ex. in $\mathbb{Z}_6$ $2 \cdot 3 = 0 = 0 \cdot 3$ but $2 \neq 0$

Def. A subset S of R is a subring of R if S is itself a ring with the operations of R

Thm (Subring test) A nonempty subset S of a ring R is a subring if S is closed under substraction and multiplication
i.e., if $a, b \in S$ then $a-b \in S$ and $ab \in S$

Ex $\{0\}$ and R are subrings of any ring R.

Ex $\{0, 2, 4\} \subseteq \mathbb{Z}_6$ is a subring
1 is the identity in $\mathbb{Z}_6$
4 is the identity in $\{0, 2, 4\}$

$\bar{0} \cdot 4 = 0 \quad 2 \times 4 = 2 \quad 4 \times 4 = 4$

Ex $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$

is a subring of $\mathbb{Z}$

does not have identity (if $n \neq 1$)