Rings

Def: A ring $(R, +, \cdot)$ is a set R with two binary operations, called addition $(+)$ and multiplication $(\cdot)$, such that

① **Additive Structure**

$(R, +)$ is a group under $+$.

so
- $+$ is associative
- $+$ is commutative
- there is an additive identity $0 \in R$
- each $a \in R$ has an additive inverse $-a \in R$

② **Multiplicative Structure**

$\cdot$ is associative.

③ **Distributive Laws**

for every $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Def: Let R be a ring.

- If R has a multiplicative identity, we call it $1 \in R$, and we say R is a <u>ring with 1</u> or ring with unity.

- If multiplication in R is commutative, then we say R is a <u>commutative ring</u>.

Ex: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings with 1.

Ex: $\mathbb{Z}_n$ (under addition and multiplication modulo n) is a commutative ring with 1.

Ex: For $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a commutative ring <u>without</u> 1, if $n > 1$.

Ex: $M_n(\mathbb{R}) = \{n \times n \text{ matrices with entries from } \mathbb{R}\}$ is a non-commutative ring with 1.

<u>Ex</u>: $\mathbb{R}[x] = \left\{ \begin{matrix} \text{polynomials in variable } x \text{ with} \\ \text{coefficients from } \mathbb{R} \end{matrix} \right\}$

is a commutative ring with 1 (under usual addition and multiplication of polynomials).

<u>Ex</u>: Polynomial rings in more variables, e.g.,

$\mathbb{R}[x,y]$, $\mathbb{R}[x,y,z]$, $\mathbb{R}[x_1, x_2, \ldots, x_n]$,

are also commutative with 1.

Basic Properties

<u>Thm</u>: Let R be a ring. Then

① $0 \cdot a = 0 = a \cdot 0$ for all $a \in R$.

② $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ for all $a, b \in R$.

③ $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in R$.

<u>Proof</u>: ① By the distributive law,

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

So $0 \cdot a = 0$ by cancellation in the group $(R, +)$.

The proof of $a \cdot 0 = 0$ is similar.

② Since

$$(-a)\cdot b + a\cdot b = ((-a)+a)\cdot b \quad \text{(Dist. Law)}$$
$$= 0\cdot b$$
$$= 0, \quad \text{(Part ①)}$$

we have that $(-a)\cdot b = -(a\cdot b)$ by uniqueness of inverses in the group $(R,+)$.

The proof of $a\cdot(-b) = -(a\cdot b)$ is similar.

③ By ②, we have

$$(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(a\cdot b))$$
$$= a\cdot b.$$

<u>Note</u>: This is <u>not</u> mult. by -1. Rather, the inverse of $-(a\cdot b)$ is $a\cdot b$.

∎

Cor: Let R be a ring with 1. Then

① $(-1)\cdot a = -a = a\cdot(-1)$ for all $a \in R$.

② $(-1)^2 = 1$.

Proof: By part ② of the previous theorem,

$$(-1)\cdot a = -(1\cdot a) = -a$$

and

$$a\cdot(-1) = -(a\cdot 1) = -a.$$

Taking $a = -1$, we get

$$(-1)^2 = -(-1) = 1.$$

$\blacksquare$

Ex: Let R be a ring with 1.
If $1 = 0$, then for all $a \in R$,

$$a = 1\cdot a = 0\cdot a = 0.$$

Hence, $R = \{0\}$ is the <u>zero ring</u>.

We will often assume $1 \neq 0$ to avoid this.

Zero divisors and units

<u>Def</u>: Let R be a ring. A non-zero element $a \in R$ is a <u>zero divisor</u> if there exists a non-zero element $b \in R$ such that

$$a \cdot b = 0 \quad \text{or} \quad b \cdot a = 0.$$

<u>Ex</u>: In $\mathbb{Z}_6$, the zero divisors are 2, 3, and 4, since $2 \cdot 3 = 4 \cdot 3 = 0$.

<u>Ex</u>: $M_n(\mathbb{R})$ has a lot of zero divisors. For instance,

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Def: Let R be a ring with 1. An element $a \in R$ which has a multiplicative inverse is called a <u>unit</u>.

Thm: Let R be a ring with identity. Then

$$R^\times := \{a \in R \mid a \text{ is a unit}\}$$

is a group (under multiplication), called the <u>group of units</u> of R.

Proof: Basically done back in Lecture 6. $\blacksquare$

Ex: $\mathbb{Z}^\times = \{1, -1\}$

$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

$(\mathbb{Z}_n)^\times = U(n)$