# Lecture XXXV: Basics on Ring Theory

**NEXT GOAL:** Study a new algebraic construction (rings) which are obtained from abelian groups

## §35.1 Basic definitions:

**Definition:** A *ring* $R$ is a (non-empty) set together with two binary operations

$+, \cdot : R \times R \longrightarrow R$ (called addition and multiplication, respectively)

and two distinct elements $0, 1 \in R$ such that:

(I) $(R, +, 0)$ is an abelian group. That is:

(i) $(a+b)+c = a+(b+c)$ $\quad \forall a,b,c \in R$ $\quad$ [Associativity of $+$]

(ii) $0+a = a+0 = 0$ $\quad \forall a \in R$ $\quad$ [0 is Neutral Element for $+$]

(iii) $\forall a \in R$, there exists an element $b \in R$ such that $a+b = 0 = b+a$. [Additive Inverses]

(iv) $a+b = b+a$ $\quad \forall a,b \in R$ $\quad$ [Abelian group]

(II) Multiplication is also an associative operation, and $1 \in R$ is neutral for multiplication

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\quad \forall a,b,c \in R$ $\quad$ [Associativity of $\cdot$]

(ii) $1 \cdot a = a = a \cdot 1$ $\quad \forall a \in R$ $\quad$ [1 is Neutral Element for $\cdot$]

⚠ We do NOT impose
- existence of multiplicative inverse ($a^{-1}$)
- commutativity for multiplication ($a \cdot b = b \cdot a$)

(III) Multiplication distributes over addition

$$a \cdot (b+c) = a \cdot b + a \cdot c \qquad \forall a,b,c \in R$$
$$(b+c) \cdot a = b \cdot a + c \cdot a \qquad \text{———}$$

## §35.2 Examples of Rings:

① $R = \mathbb{R}$ set of real numbers with usual addition and multiplication, 0 & 1 as usual

② $R = \mathbb{Z}$ (same operations as ①: restricted to $\mathbb{Z}$)

③ $R = \mathbb{Z}/n\mathbb{Z}$ $\quad n \geq 2$ $\quad$ ($+, \cdot$ = addition and multiplication modulo $n$)

④ $R = \mathcal{M}_{2\times 2}(\mathbb{C})$ = set of $2\times 2$ matrices with entries from $\mathbb{C}$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \qquad 0_R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \qquad 1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

⑤ $R = \mathbb{Z}[x]$ polynomial ring in one variable with coefficients from $\mathbb{Z}$

A typical element $f \in R$ has the form $f = a_0 + a_1 x + a_2 x^2 + \dots + a_N x^N$ for some $N \geq 0$

If $a_N \neq 0$, we call $N$ the <u>degree</u> of the polynomial $f$

<u>Convention</u>: $\deg(0) = -\infty$

- Addition of polynomials is done "component-wise" eg

$$(1+2x+3x^9) + (2+7x^3+x^{10}) = 3+2x+7x^3+3x^9+x^{10}.$$

- Multiplication of polynomials is carried out using distribution with the convention $x^n \cdot x^m = x^{n+m}$

E.g. $(1+3x)(1+5x^2+x^3) = 1\,(1+5x^2+x^3) + 3x\,(1+5x^2+x^3)$
$= 1+5x^2+x^3 + 3x + 15x^3 + 3x^4$
$= 1 + 3x + 5x^2 + 16x^3 + 3x^4$

In symbols: $(a_0 + a_1 x + \dots + a_N x^N)(b_0 + b_1 x + \dots + b_M x^M)$
$= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_2) x^2 + \dots$
$\dots + (a_0 b_\ell + a_1 b_{\ell-1} + \dots + a_\ell b_0) x^\ell + \dots + a_N b_M x^{N+M}$

$$\left(\sum_{i=0}^{N} a_i x^i\right)\left(\sum_{j=0}^{M} b_j x^j\right) = \sum_{k=0}^{N+M} \Big( \sum_{\substack{0 \leq i \leq N \\ 0 \leq j \leq M \\ i+j=k}} a_i b_j \Big) x^k$$

⑥ $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a+bi : a,b \in \mathbb{Z}\}$

Multiplication: $(a+bi)(c+di) = (ac-bd) + (ad+bc)i$

Addition: $(a+bi) + (c+di) = (a+c) + (b+d)i$

We obtain this ring as a quotient of $\mathbb{Z}[x]$ (i.e. we have the same structure as that of $\mathbb{Z}[x]$ <u>and</u> an additional rule saying $x^2 = -1$)

<u>Some remarks on these examples</u>:

- ④, ⑤ & ⑥ are quite general ways of building new rings from old ones:

$R$: ring $n \in \mathbb{Z}_{\geq 1}$ $\rightsquigarrow$ $\mathcal{M}_{n \times n}(R)$ is another ring.

$R$: ring $\rightsquigarrow$ $R[x]$ polynomial ring in one variable with coefficients from $R$.

(E.g. $R = \mathbb{Z}[x]$ $\rightsquigarrow$ $\mathbb{Z}[x_1, x_2, \dots, x_n]$ : polynomial ring in $n$ variables with coefficients from $\mathbb{Z}$.

- ①: fields are special kind of rings
  $\hookrightarrow$ • is commutative & every $a \in R \setminus \{0\}$ has a multiplicative inverse.

- ③ & ⑥: "quotient rings" $\to$ we'll introduce them later.

## §35.3 Some elementary facts and terminology:

**Lemma:** Let $R$ be a ring. For any $a \in R$ we have $a \cdot 0 = 0 \cdot a = 0$

**Proof:** $a \cdot 0 = a \cdot (0+0) \underset{\substack{\uparrow \\ \text{Distributive}}}{=} a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot 0$

Similarly, $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a + 0 \cdot a - 0 \cdot a = 0 \cdot a$ $\square$

**Definition:** An element $a \in R$ is said to be invertible (multiplicatively) if we have $b \in R$ such that $a \cdot b = 1 = b \cdot a$

Set $R^\times :=$ set of all invertible elements of $R$
$= \{a \in R : \exists\, b \in R \text{ with } a \cdot b = b \cdot a = 1_R\}$

Then, $R^\times$ is again a group (not necessarily abelian) under multiplication borrowed from $R$ [easy exercise!]

**Examples:** (i) $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ (every non-zero element has an inverse)

(ii) $\mathbb{Z}^\times = \{\pm 1\}$

(iii) $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \{x \in \{0,1,\dots,n-1\} : \gcd(x,n) = 1\}$

(iv) $\left(M_{2\times 2}(\mathbb{C})\right)^\times = GL_2(\mathbb{C})$

## §35.4 Another example:

Let $H$ be an abelian group

$R =$ set of all group homomorphisms $H \xrightarrow{f} H$.

Addition: $(f_1 + f_2)(h) = f_1(h) +_H f_2(h)$ $\forall f_1, f_2 \in R$ $\forall h \in H$

$\mathbb{0}$: constant zero function $\mathbb{0}(h) = 0_H$ $\forall h \in H$

Multiplication: composition

$(f_1 \cdot f_2)(h) = f_1(f_2(h))$

$\mathbb{1} = id_H$

**Notation:** $R = End_{gp}(H)$ "endomorphisms of $H$"

$End_{gp}(H)^\times = Aut_{gp}(H)$ "automorphisms of $H$"

## § 35.6 More terminology:

Fix $R$ a ring

**Definition:** • $R$ is commutative if $a\cdot b = b\cdot a \quad \forall\, a,b\in R$

• An element $a\in R$ is said to be a zero-divisor if we can find a non-zero element $b\in R\setminus\{0\}$ such that $b\cdot a = 0$

Examples: • $\bar{2}\in \mathbb{Z}/6\mathbb{Z}$ is a zero-divisor because $\bar{3}\neq\bar{0}$ & $\bar{3}\cdot\bar{2}=\bar{0}$

• $0_R\in R$ is always a zero-divisor because $0_R\cdot 1_R = 0_R$ & $1_R\neq 0_R$

• A commutative ring $R$ is said to be an integral domain if $0\in R$ is the only zero-divisor.

Meaning: in an integral domain $R$ $\quad a\cdot b=0$ and $a\neq 0 \implies b=0$.

( Example: $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Q}$, $\mathbb{R}$ integral domains.

$\mathbb{Z}/n\mathbb{Z}$ is not an integral domain if $n$ is not prime. )

**Lemma:** If $R$ is a commutative ring and $a\in R^\times$, then $a$ is not a zero divisor.

**Proof:** As $a\in R^\times$, we have $b\in R^\times$ such that $ab=1_R$

Now, if $a$ is a zero-divisor we must have some $y\in R$, $y\neq 0$ with $a\cdot y=0$

But then
$$\left.\begin{array}{l} b\,a\,y = b\cdot 0 = 0 \\ \quad\;\, \| \\ a\,b\,y = 1\cdot y = y \end{array}\right\} \Rightarrow y=0 \quad \text{Contradiction.}$$

$\square$

• A field is a commutative ring $R$ where $R^\times = R\setminus\{0\}$.

**Corollary:** Every field is an integral domain.

## § 35.7 Strange situations in non-commutative setting - an example:

Let $H$ be the following abelian group:

$H = \{ (a_1, a_2, \dots, a_n, \dots) \quad \text{where } a_1, a_2, \dots \in \mathbb{Z} \}$

It is a group with component-wise addition.

We consider $R = \mathrm{End}_{gp}(H)$ = set of all group homomorphisms $H \xrightarrow{f} H$

$(f_1+f_2)(h) = f_1(h)+f_2(h) \qquad\qquad 0_R(h) = (0,0,\dots) \quad \forall h\in H$

$(f_1\cdot f_2)(h) = f_1(f_2(h)) \qquad\qquad 1_R(h) = h \quad \forall h\in H$

Take $\varphi : H \longrightarrow H$ $\quad (a_1, a_2, \dots) \longmapsto (0, a_1, a_2, \dots)$ Injective but NOT surjective.

- If we take $\Psi : H \longrightarrow H$ $\quad (a_1, a_2, \dots) \longmapsto (a_2, a_3, \dots)$, then we have $\Psi \circ \varphi = 1_R$; so $\varphi$ has a left-inverse.

- If we have $\pi_1 : H \longrightarrow H$ $\quad (a_1, a_2, \dots) \longmapsto (a_1, 0, 0, \dots)$, then we have $\pi_1 \circ \varphi = 0_R$ but $\pi_1 \neq 0_R$, so $\varphi$ has a left zero-divisor.

Thus, when dealing with absolute generality, we must be careful.
We have an element that is left-invertible but has a left zero-divisor.
We will not dwell into this for our course, and hence treat the notion of zero-divisor, in particular, for commutative rings only.