

18. RINGS AND FIELDS

Definition 18.1. A **ring** $(R, +, \cdot)$ is a set R with two binary operations: addition $+$ and multiplication \cdot so that

- (1) $(R, +)$ is an additive group.
- (2) Multiplication is associative.
- (3) Multiplication distributes over addition on both sides, i.e.:

$$a(x + y) = ax + ay$$

$$(x + y)b = xb + yb$$

Example 18.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings with the usual operations of addition and multiplication. We will assume that multiplication is associative and distributive over addition without proof for these common rings. These rings are all commutative rings.

Definition 18.3. A **commutative ring** is ring R in which the multiplication is commutative: $ab = ba$ for all $a, b \in R$. (Addition is always commutative.)

Example 18.4. $M_n(\mathbb{R})$ is the ring of all $n \times n$ matrices with coefficients in \mathbb{R} . This is a ring with matrix addition

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})_{ij}$$

and matrix multiplication:

$$(a_{ij})(b_{ij}) = \left(\sum_{j=1}^n a_{ij}b_{jk} \right)_{ik}$$

The notation is that $(xxx)_{ij}$ is the matrix whose ij entry is the thing written in xxx . A more precise, rigorous definition is: $AB = C$ where the entries of C in terms of the entries of A, B are:

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$$

The ring $M_n(\mathbb{R})$ is not commutative for $n \geq 2$. For example:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proposition 18.5. If R is any ring then $M_n(R)$, the set of $n \times n$ matrices with coefficients in R

But these rings all have unity.

Definition 18.6. A ring with **unity** is a ring containing an element 1 which is the multiplicative identity:

$$1x = x1 = x$$

for all $x \in R$. Unity is unique if it exists.

In the case of $M_n(\mathbb{R})$ it is the $n \times n$ identity matrix I_n . For an arbitrary ring R , $M_n(R)$ has unity if and only if R has unity.

Definition 18.7. If R is a ring with unity then a **unit** in R is defined to be an element $u \in R$ which has a two-sided multiplicative inverse: u^{-1} :

$$u^{-1}u = 1 = uu^{-1}$$

The inverse is unique if it exists.

Example 18.8. In the ring $(\mathbb{Z}_6, +_6, \cdot_6)$ the elements are: $0, 1, 2, 3, 4, 5$. Of these 0 is the zero (additive identity) 1 is unity, 5 is a unit since $5 \cdot 5 = 1$ and the others are zero divisors since $2 \cdot 3 = 0$ and $3 \cdot 4 = 0$.

Definition 18.9. If $ab = 0$ in a ring then a, b are called **zero divisors**. a is a **left zero divisor** and b is a **right zero divisor**.

A **left annihilator** for the ring R is an element $x \in R$ so that $xy = 0$ for all $y \in R$. *right annihilators* are defined analogously. Usually annihilators are defined for subsets of R . For example, 3 is an annihilator for the subset $\{0, 2, 4\}$ of \mathbb{Z}_6 in the example above.

I also gave a very abstract example, the endomorphism ring of an additive group.

Definition 18.10. An **endomorphism** of an additive group A is defined to be a homomorphism $\phi : A \rightarrow A$. The **endomorphism ring** $\text{End}(A)$ of A is the set of all endomorphisms of A with

- (1) Multiplication given by composition: $\phi\psi := \phi \circ \psi$
- (2) Addition defined pointwise: $(\phi + \psi)(a) = \phi(a) + \psi(a)$

Theorem 18.11. The endomorphism ring of A is a ring with unity.