

Table of Contents

- 0. Preliminaries
 - Resources Used
 - Notation
- 1. Rings
 - Def. Ring
 - Thm. Basic Ring Properties
 - Thm. Basic Ring with Unity Properties
 - Def. Zero-Divisor
 - Def. Nilpotent Element
 - Def. Idempotent Element
 - Thm. (Binomial Theorem)
 - Def. Integral Domain
 - Thm. '
 - Def. Division Ring
 - Def. Field
 - Thm. On Integral Domains, Division Rings, and Fields
 - Thm. Basic Idempotent Properties
- 2. Subrings
 - Def. Subring
 - Def. Maximal Subring
 - Def. Opposite Ring
 - Thm. Self-Opposite iff Commutative
- 3. Ring Examples
 - Def. Ring of Continuous Functions
 - Example
 - Def. Matrix Ring
 - Def. Ring of Polynomials
 - Thm. Integral Domain Polynomials Properties
 - Def. Power Series Ring
 - Def. Boolean Ring
 - Thm. Structure Theorem for Boolean Rings
 - Def. Group Rings
- 5. Ideals
 - Def. Ideal
 - Def. Maximal Ideal
 - Def. Minimal Ideal
 - Thm. Existence of Maximal Ideal
 - Def. Prime Ideal
 - Thm. Nilpotents of a Commutative Ring
 - Thm. Prime Avoidance Lemma
- 4. Ring Characteristic
 - Def. Characteristic

- Thm. Basic Characteristic Properties
- Example. Characteristic Examples
- Thm. Characteristic of Cartesian Product Ring
- Thm. '

0. Preliminaries

Resources Used

- **Group Theory** notes by me, howion,
- **Introduction to Rings and Modules**, 2nd Revised Ed., by C. Musili,
- **Algebra** by Thomas W. Hungerford,
- **Abstract Algebra**, 3rd Ed., by David S. Dummit and Richard M. Foote.

Notation

- $0 \in \mathbb{N}$ and $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.
- (m, n) denotes the **greatest common divisor** of m and n .

1. Rings

From now on, knowledge of the Group Theory notes are assumed.

Def. Ring

A set R with two binary operations $+$ and \cdot , respectively called **addition** and **multiplication**, is called a **ring** if:

- $(R, +, 0)$ is an abelian group,
- (R, \cdot) is a semigroup, and
- Distribute laws hold for $+$ and \cdot .

Notice R is necessarily non-empty as the additive identity $0 \in R$.

A ring is said to be **commutative** (but not abelian) if the semigroup is commutative.

If the semigroup has an identity (that is, if the multiplication is a monoid) then its identity, denoted with 1 or 1_R , is called the **identity element** or the **unity** (of the ring). Such identity is always unique (exercise).

If the ring is with unity, then an element $u \in R$ is said to be **unit** or **invertible** if there exists $v \in R$ such that $uv = vu = 1$. Such v is unique and is called **multiplicative inverse** (or simply **inverse**) of u and is denoted with u^{-1} .

Do not mistake unity with unit. There may be one unique unit and if there is there may be many units.

The **set of all units** in the ring R is denoted by $\mathcal{U}(R)$.

The **set of all non-zero elements** of R is denoted by R^* .

The multiplication is called **trivial** if for all $a, b \in R$ we have $ab = 0$.

Thm. Basic Ring Properties

Let R be a ring, then

- The 0 is never an unit unless $0 = 1$.
- $0 = 1$ only if $R = \{0 = 1\}$, the **trivial ring** or the **zero ring**.

For all $a, b \in R$

- $0a = 0 = a0$.
- $-(a \cdot b) = (-a)b = a(-b)$.
- $(-a)(-b) = ab$

For all $m, n \in \mathbb{Z}$

- $n(ab) = (na)b = a(nb)$.
- $(mn)a = m(na) = n(ma)$.

► **Proof**

Thm. Basic Ring with Unity Properties

Let R be a ring with unity. Then

1. If u and v are units in R , then so is uv and $(uv)^{-1} = v^{-1}u^{-1}$.
2. $\mathcal{U}(R)$ is a group under multiplication, called the **group of units of R** .
3. Unless the ring is trivial, 0 is never a unit.

Def. Zero-Divisor

Let R be a ring and $a \in R$. Then a is called a **left zero-divisor** if there exists $0 \neq b \in R$ such that $ab = 0$. It is defined analogously for the **right zero-divisor**.

If a is either left or right zero-divisor, then it is said to be a **zero divisor**.

Def. Nilpotent Element

Let R be a ring and $a \in R$. Then a is said to be **nilpotent** if there exists a positive integer n such that $a^n = 0$.

Note that in any ring 0 is nilpotent which is called the **trivial nilpotent element**.

Def. Idempotent Element

Let R be a ring and $a \in R$. Then a is said to be **idempotent** if $a^2 = a$.

Similarly, in any ring 0 and, if exists, 1 are idempotent which are called **trivial idempotents**.

We say two idempotent elements are **orthogonal** to each other if $ab = ba = 0$.

Thm. (Binomial Theorem)

Let R be a ring with identity, $n \in \mathbb{N}^+$ and for $a, b \in R$ we have $ab = ba$, then

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Def. Integral Domain

A non-zero ring R is called an **integral domain** if it has no non-trivial zero-divisors.

Thm. '

Let R be an integral domain, and $a, b, c \in R$. If $ab = ac$, then either $a = 0$ or $b = c$.

Def. Division Ring

A ring $(R, +, \cdot)$ is called an **division ring** (or a **skew-field**) if, equivalently

1. $(R \setminus \{0\}, \cdot)$ forms a group, or
2. Every non-zero element of R , denoted R^* , has a multiplicative inverse.

Def. Field

A ring $(R, +, \cdot)$ is called a **field** if, equivalently (exercise)

1. It is a commutative division ring, or
2. R^* is abelian under multiplication.
3. It is a finite integral domain.

Thm. On Integral Domains, Division Rings, and Fields

Let R be a ring. Then

1. If R is a field, then it is a division ring.
2. If R is a division ring, then it is an integral domain.
3. If R is a division ring, then multiplicative cancellation holds for non-zero elements.
4. If R is an integral domain with unit, then only idempotent elements are 0 and 1.

Thm. Basic Idempotent Properties

Let R be a ring, and $a \in R$ idempotent. Then

1. $1 - a$ is idempotent as well.
2. If a is non-trivial, it is a zero-divisor as well. This shows that integral domains and division rings do not have such idempotents.

2. Subrings

Def. Subring

Let $(R, +, \cdot)$ be a ring and S a non-empty subset of R . Then $(S, +, \cdot)$ is called a subring if:

- $(S, +)$ is a subgroup of $(R, +)$, and
- (S, \cdot) is a sub-semigroup of (R, \cdot) .

$\{0\}$ and R are called the **trivial subrings**.

The **center of R** is, similar to groups, defined as

$$Z(R) = \{r \in R \mid rx = xr \text{ for all } x \in R\}$$

is a subring, and any subring of $Z(R)$ is called a **central subring**.

Beware that existence of unity in subring or the ring does not imply existence of unity in the other. Indeed, if they both have unity, they are not necessarily equal.

Same issue is also true for the units. Remember, for multiplication operation, we are assuming sub-semigroup not subgroup.

Def. Maximal Subring

Let R a ring and S a subring of R , then S is said to be **maximal subring** if $S \neq R$ and for any subring T of R we have

$$S \subseteq T \subseteq R \implies T = S \vee T = R$$

Notice how we exclude the ring itself to be called maximal subring in itself.

Def. Opposite Ring

Given a ring R , the **opposite ring** is the ring with the same set of elements and same additive operation but multiplication reversed.

Thm. Self-Opposite iff Commutative

A ring R is its **self-opposite** (isomorphic to its opposite) if and only if R is commutative.

3. Ring Examples

Def. Ring of Continuous Functions

Let R be the set of real valued continuous functions from the topological space X to \mathbb{R} . For $f, g \in R$, define the pointwise operations for all $x \in X$ as

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x)\end{aligned}$$

Then R is a commutative ring with unity where the additive identity is the constant map $\mathbf{0}$ and the unity is the constant map $\mathbf{1}$.

Example

Def. Matrix Ring

Def. Ring of Polynomials

Let R be a ring and x an *indeterminate* or *variable* over R . Define the set called **ring of polynomials over R** as

$$R[x] = \{ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in R, n \in \mathbb{N}^* \}$$

We could have actually wrote $n \in \mathbb{N}$ since $X^0 = 1$, but we don't know if R is with identity.

then $R[x]$ is a ring where addition and multiplication defined as expected over polynomials. Notice how elements of $R[x]$ of finite length, so this a set of **finite polynomials**.

Let $a_0 + a_1x + \cdots + a_nx^n = p(x) \in R[x]$. Then

- n is called the **degree** of $p(x)$ denoted with $d(p)$. If $p(x)$ is the zero polynomial it is defined to be 0,
- a_n is called the **leading coefficient** of $p(x)$,
- $p(x)$ is said to be **monic** if $a_n = 1$.

Thm. Integral Domain Polynomials Properties

Let R be an integral domain and $p(x), q(x) \in R[x]$, then

- $d(p(x)q(x)) = d(p(x)) + d(q(x))$,
- Units of $R[x]$ are the units of R ,
- $R[x]$ is also an integral domain.

Def. Power Series Ring

If we extend the definition of $R[[x]]$ to infinite polynomials, that is the set

$$F[[x]] = \{ a_0 + a_1x + a_2x^2 + \cdots \mid a_i \in R \}$$

is called the **power series over R** and is also a ring (exercise).

Def. Boolean Ring

A ring R in which every element is idempotent is called a **boolean ring**.

Thm. Structure Theorem for Boolean Rings

Every boolean ring is a subring of $\mathcal{P}(X)$, **the universal boolean ring**, for some set X .

Def. Group Rings

Let $(R, +, \cdot)$ be a commutative ring with identity $1 \neq 0$, and $(G, *) = \{ g_1, g_2, \dots, g_n \}$ a finite group. Define the **group ring RG** of G with coefficients in R as the set

$$RG = \{ a_1g_1 + a_2g_2 + \cdots + a_ng_n \mid a_i \in R \text{ and } 1 \leq i \leq n \}$$

Notice a_1g_1 multiplication is not defined.

If g_1 is the identity of G , then instead of a_1g_1 , simply, a_1 will be written.

Addition and multiplication in RG is defined componentwise on coefficients canonically. This makes RG a ring (exercise).

(Exercise) define addition (obvious) and multiplication.

5. Ideals

Def. Ideal

Let R be a ring. A subset I of R is called a **left (respectively right) ideal** of R if

1. $I \leq (R, +)$, and
2. for all $a \in R$ we have $aI \subseteq I$ (respectively $Ia \subseteq I$), under the ring multiplication.

If I is both a left and a right ideal, then it is called a **two-sided ideal** or a **2-sided ideal**. Notice that in this case we have $Ia = aI = I$.

Noting a ring R is an ideal of itself, such ideal R is called the **unit ideal**. $(0) = \{0\}$ is also an ideal in R called the **zero ideal**. These two ideals are called the **trivial ideals** of R .

Notice how the concept of an ideal is similar to the concept of a coset in group theory.

Def. Maximal Ideal

A left (resp. right or 2-sided) ideal I of a ring R is called **maximal ideal** in R if for any left (resp. right or 2-sided) ideal J of R we have

$$I \subseteq J \subseteq R \implies J = I \vee J = R$$

where $I \neq R$. Thus, we exclude unit ideal to be called maximal ideal.

Def. Minimal Ideal

Similar to maximal ideal, a left (resp. right or 2-sided) ideal of R is called a **minimal ideal** in R if for any left (resp. right or 2-sided) ideal J of R we have

$$(0) \subseteq J \subseteq I \implies J = (0) \vee J = I$$

where $I \neq (0)$. Thus, we exclude zero ideal to be called minimal ideal.

Thm. Existence of Maximal Ideal

Let R be a ring with 1 and I its left (resp. right or 2-sided) ideal such that $I \neq R$. Then there exists left (resp. right or 2-sided) maximal ideal M such that $I \subseteq M$.

This theorem need not to be true for minimal ideals even if the ring is commutative. For example, take the ring \mathbb{Z} and its ideal $2\mathbb{Z}$.

► **Proof**

Def. Prime Ideal

Also see **Wiki**: Prime Ideal.

Let R be a commutative ring and I its ideal. I is called a **prime ideal** if $I \neq R$ and for all $x, y \in R$

$$xy \in I \implies x \in I \vee y \in I.$$

Thm. Nilpotents of a Commutative Ring

The set of all nilpotent elements in a commutative ring R with 1 is the intersection of all prime ideals.

Thm. Prime Avoidance Lemma

Let R be a commutative ring, $A \leq R$, and $I_1, I_2, \dots, I_n \trianglelefteq R$ such that I_i is prime for $i \geq 3$ (that is at most two ideals are not prime). Then

If $A \not\subseteq I_j$ for any one j , then $A \not\subseteq \bigcup_{1 \leq k \leq n} I_k$. So that if A is not contained in any of the ideals, it is also not contained in their union.

4. Ring Characteristic

Def. Characteristic

Let R be any ring. The **characteristic** of R , denoted by $\text{Char}(R)$ is the least positive integer n such that $na = 0$ for all $a \in R$. If such n does not exist, then it is defined to be 0.

Thm. Basic Characteristic Properties

1. $\text{Char}(R) = 1$ if and only if $R = \langle 0 \rangle$.
2. $\text{Char}(R) = 0$ if and only if the additive order $|1|$ is infinite.
3. $\text{Char}(R) = n \neq 0$ if and only if the additive order $|1|$ is equal to n .

Example. Characteristic Examples

1. $\text{Char}(\mathbb{Z}) = \text{Char}(\mathbb{Q}) = \text{Char}(\mathbb{R}) = \text{Char}(\mathbb{C}) = \text{Char}(\mathbb{H}) = 0$,
2. $\text{Char}(M_n(R)) = \text{Char}(R)$,
3. $\text{Char}(R) = \text{Char}(R[x]) = \text{Char}(R[[x]])$,
4. $\text{Char}(\mathbb{Z}_n) = n$

► **Proof**

Thm. Characteristic of Cartesian Product Ring

Let R and S be rings, then their characteristic is

1. 0 if either R or S has characteristic 0, or
2. $\text{lcm}(\text{Char}(R), \text{Char}(S))$.

Thm. '

Suppose R is a ring with 1 whose non-units forms a subgroup under addition. Then either,

1. $\text{Char}(R) = 0$, or
2. $\text{Char}(R) = p^n$ where p prime and n positive integer.

► **Proof**

