4.3 Ring Structure

Definition 4.3.1. *A ring is a set equipped with two binary operations $(A, *, \star)$ such that*

1. *$(A, *)$ forms a commutative group with the identity denoted as 0_A.*
2. *The operation $\star$ is an associative and distributive binary operation on A with respect to $*$*

$$\forall x, y \in A,\ x \star (y * z) = x \star y * x \star z,\ \text{and}\ (x * y) \star z = x \star z * y \star z.$$

Example 4.3.2. *The sets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are well-known rings.*

Definition 4.3.3. *(Types of rings)*

1. *A ring $(A, *, \star)$ is said **Ring with unity** if its multiplicative identity exists i.e.,*

$$\exists 1_A \in A,\ 1_A \star x = x \star 1_A = x,\ \forall x \in A.$$

2. *A ring $(A, *, \star)$ is said **Commutative ring** (or abelian ring) if the operation $\star$ is commutative.*

Remark 4.3.4.
1. *If the operation $\star$ is commutative, the ring is called a commutative or abelian ring.*
2. *The set $A - \{0_A\}$ is denoted A^*.*
3. *For simplicity, we temporarily omit the notations $\star$ and $*$ defined on A in favor of the notations additive $(+)$ and multiplicative $(\times)$. So we refer to the ring $(A, +, \times)$ instead of $(A, *, \star)$.*

Definition 4.3.5.
1. *A commutative ring $(A, +, \times)$ is called integral if it is*
   - **(a)** *different from the zero ring (i.e., if $A \neq \{0_A\}$),*
   - **(b)** $\forall a, b \in A,\ (a \times b = 0) \Rightarrow (a = 0 \vee b = 0)$.

2. *When a product $a \times b$ is zero but neither a nor b is zero, we say that a and b are zero divisors.*

Example 4.3.6.

- *$(\mathbb{Z}, +, \times)$ of integers is integral, it has no zero divisors.*
- *The ring $\mathbb{Z}/6\mathbb{Z}$ of residue classes modulo 6 is not integral since $\dot{2}\dot{\times}\dot{3} = \dot{6}$, so $\dot{2}\dot{\times}\dot{3} = \dot{0}$. The same applies to $\mathbb{Z}/4\mathbb{Z}$.*

Definition 4.3.7. *Let $(A, +, \times)$ be a ring, (not necessarily commutative) and 0_A be the zero of the ring. An element $a \in A$ is said nilpotent if*

$$\exists n \in \mathbb{N}^*,\ a^n = 0_A.$$

Remark 4.3.8.

1. *$(A, +, \times)$ be a ring, (not necessarily commutative), then it is clear that a nilpotent element of A is a zero divisor.*
2. *Every ring has at least a nilpotent element which is 0_A.*

Proposition 4.3.9. *Let $(A, +, \times)$ be a ring. The computation rules in rings are as follows*

1. *$\forall x \in A$, $x \times 0_A = 0_A \times x = 0_A$ (The element 0_A is then called an absorbing element for the law $\times$.)*
2. *$\forall x, y \in A$, $(-x) \times y = x \times (-y) = -(x \times y)$.*
3. *$\forall x \in A,\ (-1_A) \times x = -x$.*
4. *$\forall x, y \in A$, $(-x) \times (-y) = x \times y$.*
5. *$\forall x, y, z \in A$, $x \times (y - z) = x \times y - x \times z$ and $(y - z) \times x = y \times x - z \times x$.*

Notations and Conventions. Let $(A, *, \star)$ be a ring. Let n be a non-zero natural number, and let x be an element of A.

1. We denote the element nx in A, which is equal to the composition by the first law $*$ of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,

$$nx = \underbrace{x * x * x * ... * x}_{n\ terms}$$

In particular, taking $n = 1$, we have $1x = x$ for all $x \in A$.

2. Similarly, we denote the element x^n in A, which is equal to the composition by the second law $\star$ of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,

$$x^n = \underbrace{x \star x \star x \star ... \star x}_{n \ terms}$$

In particular, taking $n = 1$, we have: $x^1 = x$ for all $x \in A$.

3. And for $n = 0$? Let's denote by 0_A the zero element and by 1_A the unit element of $(A, *, \star)$ (this notation is a bit unfortunate here as it reminds us of the additive notation and the multiplicative notation that we are trying to avoid). Then, by convention, for all $x \in A$, $0x = 0_A$ and $x^0 = 1_A$.

4.3.1 Sub-rings

Definition 4.3.10. *Let $(A, *, \star)$ be a ring. A non-empty subset A_1 of A is a sub-ring of A if the laws $*$ and $\star$ induce binary operations on A_1, and equipped with these laws, $(A_1, *, \star)$ is a ring.*

Proposition 4.3.11. *A non-empty subset A_1 of A is a sub-ring of A if and only if*

1. $0_A \in A_1$;
2. *For all $x, y \in A_1$, $x * y^{-1} \in A_1$;*
3. $\forall x, y \in A_1,\ x \star y \in A_1$.

Example 4.3.12. *$(\mathbb{Z}, +, \times)$ is a sub-ring of $(\mathbb{Q}, +, \times)$, which is a sub-ring of $(\mathbb{R}, +, \times)$, and that is a sub-ring of $(\mathbb{C}, +, \times)$.*

4.3.2 Ring Homomorphisms

Definition 4.3.13. *Let $(A, +_A, \times_A)$ and $(B, +_B, \times_B)$ be two rings with unity. A ring homomorphism from A to B is a function from A to B such that*

1. $f(1_A) = 1_B$;
2. *For all $x, y \in A$, $f(x +_A y) = f(x) +_B f(y)$, and $f(x \times_A y) = f(x) \times_B f(y)$.*

4.3.3 Ideals of a Commutative Ring

Let $(A, +, \times)$ be a commutative ring

Definition 4.3.14. *(Ideal) A subset I of A is an ideal of the ring $(A, +, \times)$ if*

1. *$(I, +)$ is a subgroup of $(A, +)$;*

2. *For every $a \in A$, we have $aI \subset I$, in other words $\forall a \in A$, $\forall x \in I$: $ax \in I$.*

Proposition 4.3.15. *A subset I of A is an ideal of the ring $(A, +, \times)$ if and only if*

1. *$0_A \in I$;*

2. *For all $x, y \in I$, $x - y \in I$.*

3. *$\forall a \in A$, $\forall x \in I$, $a \times x \in I$.*

Examples 4.3.16.

1. *Every non-trivial ring has at least two ideals: the trivial ideal $\{0\}$ and A itself. The ideals of A, distinct from A, are called proper ideals.*

2. *Every element x of A defines a principal ideal*

$$< x >= xA = \{ax / a \in A\}.$$

It is the smallest ideal that contains a, and we say it is generated by a.

3. *More generally, if $x_1, x_2, ..., x_n$ belong to A, the smallest ideal containing $x_1, x_2, ..., x_n$ is*

$$< x_1, x_2, ..., x_n >= x_1A + x_2A + ... + x_nA = \{a_1x_1 + ... + a_nx_n / a_1, ..., a_n \in A\}.$$

Indeed, it is immediately verified that $I = x_1A + x_2A + ... + x_nA$ is non-empty and stable under linear combinations, therefore it is an ideal.

4.4 Field Structure

Definition 4.4.1. *A field is a commutative ring in which every non-zero element is invertible.*

If, in addition, the second operation $\times$ is commutative on $\mathbb{K}$, then we say that the field $(\mathbb{K}, +, \times)$ is commutative.

Example 4.4.2. *$(\mathbb{Q}, +, \times)$ and $(\mathbb{R}, +, \times)$ are commutative fields.*

$(\mathbb{Q}, +, \times)$ is not a field.