INTRODUCTION

Modern algebra, also called abstract algebra, the branch of mathematics concerned with the general algebraic structure of various sets (such as real numbers, complex numbers, matrices and vector spaces) rather than rules and procedures for manipulating their individual elements. In algebra, the board division of mathematics, abstract algebra includes the study of algebraic structures like group, ring, fields, homomorphism etc. Abstract algebra has an interesting way of making a problem more transparent by forgetting about superfluous properties. Because of its generality, abstract algebra is used in many fields of mathematics and science.

We have already studied that the set of integers, denoted as $\mathbb{Z}$ consists of zero(0), the positive natural numbers $(1,2,3,..)$ also called the whole numbers or counting numbers, and their additive inverses(the negative integers ,ie$-1,-2,-3,..$)

Our project is mainly focusing on the ideal features carrying by the set of all integers in abstract algebra with the proper analysis of corresponding examples.

CHAPTER 1
PRELIMINARIES

GROUP

A non empty set S along with an operation $*$ is called an algebraic structure. It is denoted by $(S,*)$.

For example, the set of all integers $\mathbb{Z}$ under usual addition is an algebraic structure and is denoted by $(\mathbb{Z},+)$.

Now consider an algebraic structure $(S,*)$

If $a * b \in S, \forall a, b \in S,$ then we say $*$ is a binary operation on S.

For example, the operation usual addition $+$ is a binary operation on the sets $\mathbb{Z}, \mathbb{N}, \mathbb{R}$.

That is, let $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$. And similarly in case of $\mathbb{N}, \mathbb{R}$.

But the operation usual substraction '$-$' is not binary in the set of all natural numbers $\mathbb{N}$ since for $2{,}3 \in \mathbb{N}$, $2 - 3 = -1 \notin \mathbb{N}$.

The operation $*$ is associative on S if $(a * b) * c = a * (b * c)\ \forall a, b, c \in S$.

In $(\mathbb{Z},+)$, $a + (b + c) = (a + b) + c \ \forall a, b, c \in \mathbb{Z}$.

But usual substraction '$-$' is not associative in the set of all rational numbers $\mathbb{Q}$ since for

$1{,}2{,}3 \in \mathbb{Q}\ (1 - 2) - 3 \neq 1 - (2 - 3)$.

The operation $*$ is commutative on S if $a * b = b * a \ \forall a, b \in S$.

Since $a + b = b + a\ \forall a, b \in \mathbb{Z}$, the usual addition is commutative on $\mathbb{Z}$.

But usual substraction '$-$' is not commutative in $\mathbb{R}$ since $2 - 3 \neq 3 - 2$ for $2{,}3 \in \mathbb{R}$.

A **Group** is an algebraic structure $(G,*)$ satisfying the following conditions:

I. $*$ is a binary operation on G

II. $*$ is associative on G

III. Condition for existence of identity element

There exist an element $e \in G$ such that $e * x = x = x * e, \forall x \in G$.

The element $\boldsymbol{e}$ is called **identity element** of G with respect to $*$

IV. Condition for existence of inverse element

For each $a \in G, \exists$ an element $b \in G$ such that $a * b = e = b * a$.

The element b is called **inverse** of a and is denoted by a^{-1}.

Then $(G,*)$ is a group.

A Group $(G,*)$ is an **Abilean group** or **Commutative group** if $*$ is commutative on G.

Examples:

- $(\mathbb{Z}, +)$ is an Abelian group.

  The operation usual addition is binary on the set of all integers $\mathbb{Z}$ and is associative in $\mathbb{Z}$.

  Since $\exists$ an element $0 \in \mathbb{Z}$ such that $a + 0 = a = 0 + a \; \forall \; a \in \mathbb{Z}$.That is 0 is the identity element in $\mathbb{Z}$ under $+$.

  For each $a \in \mathbb{Z}$, there exist an element $(-a) \in \mathbb{Z}$ such that

  $$a + (-a) = 0 = (-a) + a.$$

  That is, $-a$ is the inverse of a.
- $(\mathbb{Z},\times)$is not an Abelian group since condition for existence of inverse element is not satisfied.
- Consider the set of all whole numbers, W. Then $W$is not an Abelian group under usual addition since condition for existence of inverse element is not satisfied.
- $(\mathbb{Q}, +)$is an Abelian group.

Addition modulo m, $+_{\boldsymbol{m}}$

Let a and b be two integers.By addition modulo m we mean the least nonnegative number r where r is the remainder when sum $a + b$ is divided by m. It is denoted by $a +_{\boldsymbol{m}} b$.

The set $\mathbb{Z}_n$under addition modulo n:

We denote $\mathbb{Z}_n = \{0,1,2,3, \dots, n-1\}$.

The set $\mathbb{Z}_n$ is an abelian group under addition modulo n.

The operation $+_n$ is both binary and associative on $\mathbb{Z}_n$. Then $0 \in \mathbb{Z}_n$ is the identity element in $\mathbb{Z}_n$ under $+_n$. Also there exist inverse element for every element in $\mathbb{Z}_n$ under$+_n$.

For example, Consider $\mathbb{Z}_3 = \{0,1,2\}$ under addition modulo $+_3$. Given below is the composition table which defines the operation $+_3$ on $\mathbb{Z}_3$.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

From the table, it is clear that 0 is the identity element in $\mathbb{Z}_3$ under $+_3$. And $0^{-1} = 0$, $1^{-1} = 2$ and $2^{-1} = 1$.

Subgroup

Let $(G,*)$be a group. Let $H \subseteq G$. If H is itself a group under the induced operation from G, we say that H is a subgroup of G and is denoted by $H \leq G$.

Let $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$. Then $n\mathbb{Z} \leq \mathbb{Z}$ under usual addition.

RING

A **Ring** is an algebraic structure $(R, +,\cdot)$ consisting of a nonempty set R and two operations called addition and multiplication denoted by $+$ and $\cdot$ respectively satisfying the following conditions:

I. $+$ is binary operation on R

II. $+$ is associative on R

III. Existence of identity element with respect to $+$ in R

IV. Existence of inverse element with respect to $+$ in R

V. $+$ is commutative on R

VI. $\cdot$ is binary operation on R

VII. $\cdot$ is associative on$R$

VIII. $\cdot$ is distributive over $+$ on R

That is, for all $a, b, c \in R$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{(Left Distributive Law)}$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{(Right Distributive Law)}$$

EXAMPLES

- $(\mathbb{Z}, +,\cdot)$ is a ring where $+$ is the usual addition and . is usual multiplication. Clearly $(\mathbb{Z}, +)$ is an abelian group. Also multiplication of integers is both binary and associative. Clearly usual multiplication of real numbers is distributive over usual addition and therefore distributive law holds.
- $(\mathbb{Q}, +,\cdot)$ is a ring
- $\{a + b\sqrt{2} \ : a, b \in \mathbb{Z}\}$ is a ring with respect to ordinary multiplication and addition
- Set of all $n \times n$ matrices with real entries is a ring with respect to matrix addition and multiplication
- Set of all real valued continuous functions is a ring with respect to addition and multiplication
- Multiplication modulo m, $\times_m$, is the least non negative number r which is the remainder when the product $a \times b$ is divided by m.
  Then the structure$(\mathbb{Z}_n , +_n, \times_n)$ is a ring.

Commutative ring

A ring $(R, +,\cdot)$ in which multiplication operation is commutative is called **commutative ring.**

- $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are commutative rings.
- Ring $(\mathbb{Z}_n\ ,+_n,\times_n)$ is a commutative ring.
- The set of all matrices with real entries, $M_n(\mathbb{R})$ is not a commutative ring under matrix addition and matrix multiplication.

Ring with unity

If in a ring $(R,+,\cdot)$ there exist multiplicative identity, the ring is called **ring with unity.** The multiplicative identity in ring is called **unity** and is denoted by 1.

- $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are rings with unity
- $(\mathbb{Z}_n\ ,+_n,\times_n)$ is a ring with unity and 1 is the unity.
- $(2\mathbb{Z},+,\cdot)$ is a ring without unity

Division ring and Fields

An element in a ring is called a **unit** if it has a multiplicative inverse in that ring. If every nonzero element (except additive identity) in a ring is unit, then the ring is called a **division ring**.

- $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are examples for division rings
- $(\mathbb{Z},+,\cdot)$ is not a division ring since all nonzero elements in $\mathbb{Z}$ are not units. Only ± 1 are the units in $\mathbb{Z}$.
- $(\mathbb{Z}_n\ ,+_n,\times_n)$ is a not a division ring since every nonzero elements are not units.

  The unit elements in $(\mathbb{Z}_n\ ,+_n,\times_n)$ are nonzero elements in $\mathbb{Z}_n$ that are relatively prime to n. That is, $(\mathbb{Z}_p,+_p,\times_p)$ is a division where p is a prime.

❖ A commutative division ring is a **field.**

- $(\mathbb{Z},+,\cdot)$ is not a field
- $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are examples for field.
- $(\mathbb{Z}_n\ ,+_n,\times_n)$ is a field if n is prime number.

Divisors of zero

If a and b are two non zero elements of a ring $(R,+,\cdot)$ such that $a\cdot b=0$, then a and b are zero divisors.

- Ring $\mathbb{Z}$ has no zero divisors

  For any $a\neq 0$and $b\neq 0$, then $a\cdot b\neq 0$ in $\mathbb{Z}$.

  $\therefore$ $(\mathbb{Z},+,\cdot)$ has no zero divisors.
- Also $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are rings with no zero divisors
- The zero divisors in $(\mathbb{Z}_n\,,+_n,\times_n)$ are the elements in $\mathbb{Z}_n$ which are not relatively prime to n.
- Ring $M_n(\mathbb{R})$ has zero divisors in it.

  For example, $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$

  $\therefore$ $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}and\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$ are zero divisors in$M_2(\mathbb{R})$.

INTEGRAL DOMAIN

An **Integral domain** D is a commutative ring with unity $1\neq 0$ and containing no zero divisors.

$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$,$(\mathbb{R},+,\cdot)$,$(\mathbb{C},+,\cdot)$ are all commutative rings with unity and with no zero divisors. These are examples of integral domain.

$(\mathbb{Z}_n\,,+_n,\times_n)$ is a commutative ring with unity and has no zero divisors iff n is a prime. That is, $(\mathbb{Z}_n\,,+_n,\times_n)$ is an integral domain iff n is a prime.

Subring

A subring S of a ring R is a subset of R which is a ring itself under the same operations from R.

$n\mathbb{Z}$ is a subring of $\mathbb{Z}$ under usual addition and multiplication.

Homomorphism

A map ϕ of a group G into a group G' is a homomorphism if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds for all $a, b \in G$.

If the homomorphism ϕ is one - one and onto, then ϕ is called isomorphism. And we say G is isomorphic to G', is denoted by $G \simeq G'$.

A map ϕ of a ring R into a ring R' is a ring homomorphism if

$$\phi(a + b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\phi(b)$$

for all elements a and b in R.

COSETS

Let H be a subgroup of a group G. The subset $aH = \{ah : h \in H\}$ of G is the left coset of H containing a, while the subset $Ha = \{ha : h \in H\}$ is the right coset of H containing a.

For a subgroup H of an abelian group $G,$ the partition of G into left cosets of H and the partition into right cosets are the same.

Example

Right and left cosets of the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$.

Since $\mathbb{Z}$ is an abelian group both left and right cosets coincide. And the cosets are the following

$$0 + 3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$$1 + 3\mathbb{Z} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

$$2 + 3\mathbb{Z} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}.$$

Generally, Cosets of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ are :

$0 + n\mathbb{Z}, 1 + n\mathbb{Z}$, 2+$n\mathbb{Z}, 3 + n\mathbb{Z}$, $4 + n\mathbb{Z}$,…, (n-1)+$n\mathbb{Z}$.

CHAPTER 2

IDEALS, FACTOR RINGS AND FACTOR GROUPS

IDEALS

Ideal is a special type of subset of a ring. For a ring $(R, +, \cdot), (R, +)$ is an additive group. A subset I is called a left ideal of R if I is an additive subgroup of R that absorbs multiplication from left by elements of R. That is, I is left ideal if it satisfies following conditions:

- $(I, +) \leq (R, +)$
- For every r ∈ R and every $x \in I, rx \in I$

Similarly a right ideal is defined with conditions

- $(I, +) \leq (R, +)$
- For every r ∈ R and every $x \in I, xr \in I$

A two sided ideal is a left ideal as well as right ideal and sometimes is simply called an ideal.

A subring must be closed under multiplication of the elements in the subring .An ideal must be closed under multiplication of an element in the ideal by any element in the ring.

Every ideal in a ring is a subring of the ring. But the converse may not be true that is every subring of a ring neednotbe an ideal of the ring.

For example, ℤ is a sub ring of R,but is not an ideal .

($\mathbb{Z}, +, \cdot$)is a ring itself. That is, ℤ is subring of ℝ under induced operations.

Let $\sqrt{2} \in \mathbb{R}, 3 \in \mathbb{Z}$ but $3\sqrt{2} \notin \mathbb{Z}$. Thereforeℤ is not an ideal in ℝ

IDEALS OF $\mathbb{Z}$

1. The set of all even integers form an ideal in ring $\mathbb{Z}$, denoted by$2\mathbb{Z}$.

   Since sum of any two even integers is again an even integer $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

That is, $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

Also the product of any integer with an even integer is again an even integer.

That is, for every $m \in \mathbb{Z}$ and $2n \in 2\mathbb{Z}$

$$m(2n) = 2(mn) \in 2\mathbb{Z}$$

$$(2n)m = 2(mn) \in 2\mathbb{Z}$$

2. The set $10\mathbb{Z} = \{0, \pm 10, \pm 20, \dots\}$ form an ideal in the ring $\mathbb{Z}$

   Let $10m, 10n \in 10\mathbb{Z}$

   Then $10m + 10n = 10(m+n) \in 10\mathbb{Z}$

   That is, $(10\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

   Also for every $r \in \mathbb{Z}$ and every $10m \in 10\mathbb{Z}$

$$r(10m) = 10(rm) \in 10\mathbb{Z}$$

$$\text{And } (10m)r = 10(mr) \in 10\mathbb{Z}$$

3. In generally, Set of all integers divisible by a fixed integer n,is an ideal of ring $\mathbb{Z}$.

   That is, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is an ideal of$\mathbb{Z}$.

   Let $nm, nr \in n\mathbb{Z}$

   Then $nm + nr = n(m+r) \in n\mathbb{Z}$

   That is, $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

   Also for every $r \in \mathbb{Z}$ and every $nm \in n\mathbb{Z}$

$$r(nm) = n(rm) \in n\mathbb{Z}$$

$$\text{And } (nm)r = n(mr) \in n\mathbb{Z}$$

4. $\{0\}$ is the trivial ideal of $\mathbb{Z}$

   Clearly $(\{0\}, +) \leq (\mathbb{Z}, +)$

   Also for every $r \in \mathbb{Z}$ and $0 \in \{0\}$

$$r0 = 0 \in \{0\}$$

$$0r = 0 \in \{0\}$$

5. $\mathbb{Z}$ itself is an ideal of $\mathbb{Z}$ and is called improper ideal.

PRIME IDEALS

An ideal $N \neq R$ in a commutative ring R is a **prime ideal** if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

In case of integers :

1. $\{0\}$ is a prime ideal of $\mathbb{Z}$

   Because for any $ab \in \{0\}$ either $a = 0$ or $b = 0$
2. Ideal $5\mathbb{Z}$ is a prime ideal since the product of any two integers is a multiple of 5 only if at least one of the two is a multiple of 5
3. Ideal $6\mathbb{Z}$ is not a prime ideal

   $\because \ 2 \times 3 = 6 \in 6\mathbb{Z}$ but neither 2 nor 3 is an element of $6\mathbb{Z}$
4. Ideal $7\mathbb{Z}$ is a prime ideal since the product of any two integers is a multiple of 7 only if at least one of the two is a multiple of 7
5. Ideal $10\mathbb{Z}$ is not a prime ideal

   $\because \ 5 \times 2 = 10 \in 10\mathbb{Z}$ but neither 5 nor 2 is an element of $10\mathbb{Z}$
6. Ideal $9\mathbb{Z}$ is not a prime ideal

   $\because \ 6 \times 3 = 18 \in 9\mathbb{Z}$ but neither 6 nor 3 is an element of $9\mathbb{Z}$
7. Ideal $11\mathbb{Z}$ is a prime ideal since the product of any two integers is a multiple of 11 only if at least one of the two is a multiple of 11
8. Ideal $13\mathbb{Z}$ is a prime ideal since the product of any two integers is a multiple of 13 only if at least one of the two is a multiple of 13
9. In generally, $p\mathbb{Z}$ is a prime ideal, where p is a prime number.

MAXIMAL IDEAL

A proper ideal M of a ring R is a maximal ideal such that there is no proper ideal N of R properly containing M.

- Every maximal ideal in a commutative ring with unity is prime ideal
- Maximal ideal is an ideal M that is maximal in the set of all proper ideals in R.That is M is contained exactly in two ideals of R namely, M itself and the entire ring R.

MAXIMAL IDEALS OF $\mathbb{Z}$

1. Ideal $5\mathbb{Z}$ is a maximal ideal of Z since $5\mathbb{Z}$ is not contained in any other proper ideal of $\mathbb{Z}$
2. Ideal $9\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ since $9\mathbb{Z} \subseteq 3\mathbb{Z}$
3. Ideal $2\mathbb{Z}$ is a maximal ideal since $2\mathbb{Z}$ is not contained in any other proper ideal of $\mathbb{Z}$
4. $3\mathbb{Z}$ is a maximal ideal since $3\mathbb{Z}$ is not contained in any other proper ideal of $\mathbb{Z}$
5. $10\mathbb{Z}$ is not maximal ideal since $10\mathbb{Z} \subseteq 2\mathbb{Z}$
6. Generally $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$ where p is a prime number

THEOREM

Let R be a commutative ring with unity.Then M is a maximal ideal of R if and only if R/M is a field.

PROOF

Suppose M is a maximal ideal in R. Observe that if R is a commutative ring with unity, then $R/M$is also a nonzero commutative ring with unity if $M \neq R$, which is in case if M is maximal.Let $(a + M) \in R/M$, with $a \notin M$, so that $a + M$ is not the additive identity element in R/M. Suppose $a + M$ has no multiplicative inversein $R\ /\ M$. Then the set $(R/M)(a + M) = \{(r + M)(a + M) |\ (r + M) \in R\ /\ M\}$does not contain $1 + M$. We easily see that $(R/M)(a + M)$ is an ideal of $R\ /\ M$. It is nontrivial because $a \notin M$,and it is a proper ideal because it does not contain $1 + M$. If $\gamma : R \longrightarrow R\ /\ M$ is a homomorphism, then $\gamma^{-1}[(R/M)(a + M)]$ is a proper ideal of R properly containing M. But this contradicts our assumption that M is a maximal ideal, so $a + M$ must have a multiplicative inverse in R/M.

Conversely, suppose that $R\ /\ M$ is a field. If N is any ideal of R such that $M \subset N \subset R$ and γ is a homomorphism of R onto $R\ /\ M$, then $\gamma[N]$ is an ideal of $R\ /\ M$ with $\{(0 + M)\} \subset \gamma[N] \subset R/M$. But this is contrary to the fact that field $R\ /\ M$ contains no proper nontrivial ideals. Hence ifR/M is a field, M is maximal.

EXAMPLE: We see that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. We know that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to ring $\mathbb{Z}_p$ and that $\mathbb{Z}_p$ is actually a field. Thus $\mathbb{Z}/p\mathbb{Z}$ is a field .This illustrates the Theorem.

- ❖ All Ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. For $n = 0$, we have $n\mathbb{Z} = \{0\}$, and $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$, which is an integral domain.For $n > 0$, we have $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ and $\mathbb{Z}_n$ is field if and only if n is a prime.Thus the nonzero ideals $n\mathbb{Z}$ such that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain are of the form $p\mathbb{Z}$, where p is a prime. Of course, $\mathbb{Z}/p\mathbb{Z}$ is actually a field, so that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. Note that for a product rs of integers to be in $p\mathbb{Z}$, the prime$p$ must divide either r or s.The role of prime integers in this example makes the use of the word *prime* in the next definition more reasonable

PRINCIPAL IDEAL

The ideal generated by one element is called principal ideal in a ring.

Let R be a commutative ring with unity and $a \in R$ .The ideal $\{\boldsymbol{ra}: \boldsymbol{r} \in \boldsymbol{R}\}$ of all multiples of a is the **principal ideal** generated by a and is denoted by$\langle \boldsymbol{a} \rangle$.

An ideal N of R is a principal ideal if $N = \langle a \rangle$ for some $\in R$.

PRINCIPAL IDEALS IN $\mathbb{Z}$

1. $2\mathbb{Z}$ is a principal ideal since $2\mathbb{Z} = \langle 2 \rangle$ where $2 \in \mathbb{Z}$
2. $5\mathbb{Z}$ is a principal ideal since $5\mathbb{Z} = \langle 5 \rangle$where $5 \in \mathbb{Z}$
3. $7\mathbb{Z}$ is a principal ideal since $7\mathbb{Z} = \langle 7 \rangle$where $7 \in \mathbb{Z}$
4. $\{0\}$ is a principal ideal where $\{0\} = \langle 0 \rangle$
5. Generally every ideal of ring $\mathbb{Z}$ is principal ideal

   PROOF

   Let I be ideal in $\mathbb{Z}$.

   If$I = \{0\}$,thenclearly $I = \langle 0 \rangle$

   Therefore I is a principal ideal

   Now let $I \neq \{0\}$

Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$

Then let $I = n\mathbb{Z} = \{rn: r \in \mathbb{Z}\} = \langle n \rangle$

Therefore I is principal ideal in all cases

Every ideal of $\mathbb{Z}$ is a principal ideal.

PRINCIPAL IDEAL DOMAIN

A ring R is a **principal domain**(PID) if it is an integral domain such that every ideal of R is a principal ideal.

Ring $\mathbb{Z}$ is a PID since all of its ideal are principal ideal.

IDEALS OF $\mathbb{Z}_n$

- Ideals of $\mathbb{Z}_{12}$

$\mathbb{Z}_{12} = \{0,1,2,3, \ldots.,11\}$. The subgroups of $\mathbb{Z}_{12}$ are the following:

Subgroup generated by 2, $\langle 2 \rangle = \{0,2,4,6,8,10\}$

Subgroup generated by 3, $\langle 3 \rangle = \{0,3,6,9\}$

Subgroup generated by 4, $\langle 4 \rangle = \{0,4,8\}$

Subgroup generated by 6, $\langle 6 \rangle = \{0,6\}$

These are the proper nontrivial ideals of $\mathbb{Z}_{12}$. $\mathbb{Z}_{12}$is the improper ideal and$\langle 0 \rangle = \{0\}$ is the trivial ideal. Here ideals generated by 2 and 3,that is $\langle 2 \rangle$and $\langle 3 \rangle$are both prime and maximal ideal. But $\langle 4 \rangle$ and $\langle 6 \rangle$ are neither prime nor maximal ideal. Also the trivial ideal is not a maximal ideal.

Since $\mathbb{Z}_{12}/\langle 0 \rangle \simeq \mathbb{Z}_{12}$ and clearly $\mathbb{Z}_{12}$ is not a field. This implies $\langle 0 \rangle$ is not a maximal ideal.

Similarly,

$\mathbb{Z}_{12}/\langle 2 \rangle \simeq \mathbb{Z}_2$and $\mathbb{Z}_2$ is a field $\Longrightarrow \langle 2 \rangle$ is a maximal ideal in $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12}/\langle 3 \rangle \simeq \mathbb{Z}_3$ and$\mathbb{Z}_3$ is a field $\Longrightarrow \langle 3 \rangle$ is a maximal ideal in $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12}/\langle 4 \rangle \simeq \mathbb{Z}_4$and $\mathbb{Z}_4$ is not a field $\Longrightarrow \langle 4 \rangle$ is not a maximal ideal in $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12}/\langle 6\rangle \simeq \mathbb{Z}_6$and $\mathbb{Z}_6$ is not a field $\Longrightarrow \langle 6\rangle$ is not a maximal ideal in $\mathbb{Z}_{12}$.

- Ideals of $\mathbb{Z}_6$

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. The proper nontrivial subgroups of $\mathbb{Z}_6$ are the following:

Subgroup generated by 2, $\langle 2\rangle = \{0,2,4\}$

Subgroup generated by 3, $\langle 3\rangle = \{0,3\}$

These are the proper non trivial ideals of $\mathbb{Z}_6$. $\mathbb{Z}_6$is the improper ideal and $\langle 0\rangle = \{0\}$ is the trivial ideal. Here ideals generated by 2 and 3, that is $\langle 2\rangle$and $\langle 3\rangle$are both prime and maximal ideal. And the trivial ideal is not a maximal ideal.

Since $\mathbb{Z}_6/\langle 0\rangle \simeq \mathbb{Z}_6$ and clearly $\mathbb{Z}_6$ is not a field. This implies $\langle 0\rangle$ is not a maximal ideal.

Similarly,

$\mathbb{Z}_6/\langle 2\rangle \simeq \mathbb{Z}_2$and $\mathbb{Z}_2$ is a field $\Longrightarrow \langle 2\rangle$ is a maximal ideal in $\mathbb{Z}_{12}$.

$\mathbb{Z}_6/\langle 3\rangle \simeq \mathbb{Z}_3$and $\mathbb{Z}_3$ is a field $\Longrightarrow \langle 3\rangle$ is a maximal ideal in $\mathbb{Z}_{12}$.

FACTOR RINGS (QUOTIENT RINGS)

Let N be an ideal of the ring R. Then the additive cosets of N form a ring $R\ /\ N$ with the binary operations defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N.$$

The ring $R\ /\ N$ is the the factor ring or quotient ring of R by N.

THEOREM

Let N be an ideal of ring R, then $\gamma : R \longrightarrow R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with Kernel N.

PROOF

Clearly from the definitions of binary operations of factor rings, we have

$$\gamma(x + y) = (x + y) + N = (x + N) + (y + N) = \gamma(x) + \gamma(y)$$

$\gamma(xy) = (xy) + N = (x + N)(y + N) = \gamma(x)\gamma(y)$.

Therefore γ is a ring homomorphism.

Fundamental Homomorphism Theorem

Let $\phi : R \longrightarrow R'$ be a ring homomorphism with kernel N. Then $\phi[R]$ is a ring, and the map $\mu : R/N \longrightarrow \phi[R]$ given by $\mu(x + N) = \phi(x)$ is an isomorphism. If $\gamma : R \longrightarrow R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have $\phi(x) = \mu\gamma(x)$.

FACTOR RING OF INTEGERS

- The set of all even integers, $2\mathbb{Z} = \langle 2 \rangle$ is an ideal of $\mathbb{Z}$. So we can form quotient ring $\mathbb{Z} / 2\mathbb{Z}$.
  $\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$.
  The operations are defined by
  $$(0 + 2\mathbb{Z}) + (1 + 2\mathbb{Z}) = 1 + 2\mathbb{Z}$$
  and
  $$(0 + 2\mathbb{Z})(1 + 2\mathbb{Z}) = 0 + 2\mathbb{Z}.$$
  The two operations are essentially modulo 2 arithmetic.
  Let $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ where $\phi(m)$ is the remainder of m modulo 2 is a homomorphism, we see that Ker$(\phi) = 2\,\mathbb{Z}$. By the fundamental theorem of

homomorphism, the map $\mu : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}_2$, where $\mu(m + \ 2\ \mathbb{Z})$ is the remainder of m modulo 2 is well defined and is an isomorphism.

- The set of all multiples of 4, $4\mathbb{Z} = \langle 4 \rangle$ is an ideal of $\mathbb{Z}$. So we can form quotient ring $\mathbb{Z}$ / $4\mathbb{Z}$.

  $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z},\ 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$.

  To see how to add and multiply consider

  $$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$$

  and

  $$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 2 + 4\mathbb{Z}.$$

  The two operations are essentially modulo 4 arithmetic.

  Let $\phi : \mathbb{Z} \ \longrightarrow \mathbb{Z}_4$ where $\phi(m)$ is the remainder of m modulo 4 is a homomorphism, we see that Ker$(\phi) = 4\ \mathbb{Z}$. By the fundamental theorem of homomorphism, the map $\mu : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}_4$, where $\mu(m + \ 4\ \mathbb{Z})$ is the remainder of m modulo 4 is well defined and is an isomorphism.

- The set of all multiples of n, $n\mathbb{Z} = \langle n \rangle$ is an ideal of $\mathbb{Z}$. So we can form quotient ring $\mathbb{Z}$ / $n\mathbb{Z}$.

  $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z},\ 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$.

  Let $\phi : \mathbb{Z} \ \longrightarrow \mathbb{Z}_n$ where $\phi(m)$ is the remainder of m modulo n is a homomorphism, we see that Ker$(\phi) = n\mathbb{Z}$. By the fundamental theorem of homomorphism, the map $\mu : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n$, where $\mu(m + \ n\ \mathbb{Z})$ is the remainder of m modulo n is well defined and is an isomorphism.

FACTOR GROUPS

For a Group G and a normal subgroup $H$of G, the set of cosets of H form a group G/H under the binary operation$(aH)(bH) = (ab)H$. And the group G/H (read G modulo H) is a **factor group** of $H$in$G$ . Factor groups are also called **quotient groups.**

THEOREM

Let $\phi : G \longrightarrow G'$ be a group homomorphism with kernel H. Then the cosets of H form a factor group,G/H,where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \longrightarrow \phi[G]$

defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices of a and b from the cosets.

Consider the map $\gamma : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, where $\gamma(m)$ is the remainder when m is divided by n in accordance with the division algorithm. We know that γ is a homomorphism. Of course, $\mathrm{Ker}(\gamma) = n\mathbb{Z}$. By Theorem, We see the factor group $\mathbb{Z} \,/\, n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the residue classes modulo n.

For example, taking $n = 5$, we see the cosets of $5\mathbb{Z}$ are

$$5\mathbb{Z} = \{\cdots, -10, -5, 0, 5, 10, \cdots\},$$

$$1 + 5\mathbb{Z} = \{\cdots, -9, -4, 1, 6, 11, \cdots\},$$

$$2 + 5\mathbb{Z} = \{\cdots, -8, -3, 2, 7, 12, \cdots\},$$

$$3 + 5\mathbb{Z} = \{\cdots, -7, -2, 3, 8, 13, \cdots\},$$

$$4 + 5\mathbb{Z} = \{\cdots, -6, -1, 4, 9, 14, \cdots\}.$$

Note that the isomorphism $\mu : \mathbb{Z} \,/\, 5\mathbb{Z} \longrightarrow \mathbb{Z}_5$ of theorem assigns to each coset of $5\mathbb{Z}$ its smallest nonnegative element. That is, $\mu(5\mathbb{Z}) = 0, \mu(1 + 5\mathbb{Z}) = 1$, etc.

FACTOR GROUPS OF $\mathbb{Z}$

a) Consider the subgroup $2\mathbb{Z}$ consisting of set of all even integers. Since $\mathbb{Z}$ is abelian, $2\mathbb{Z}$ is a normal subgroup. There are only two cosets: the set of all even integers and the set of all odd integers, and therefore the factor group $\mathbb{Z} \,/\, 2\mathbb{Z}$ is the cyclic group with two elements.This quotientgroup is isomorphic to the set $\{0,1\}$ with addition modulo 2; informally it is sometimes said that $\mathbb{Z} \,/\, 2\mathbb{Z}$ equals the set $\{0,1\}$ with addition modulo 2.
Further explanation of the example,
Let $\phi(m)$ =remainder of $m \in \mathbb{Z}$ when divided by 2.
Then $\phi(m) = 0$ when m is even and $\phi(m) = 1$ when m is odd.
By the definition of ϕ, Kernel of ϕ, $\mathrm{Ker}(\phi) = \{m \in \mathbb{Z} : \phi(m) = 0\}$, is the set of all even integers.

Let H =Ker(ϕ).Then, H is a subgroup, because the identity in $\mathbb{Z}$, which is 0, is in H, the sum of two even integers is even (closure) and if m is even, $-m$ is also even and so H contains its inverses.

Define $\mu : \mathbb{Z} / H \longrightarrow \mathbb{Z}_2$ as $\mu(aH) = \phi(a)$ for $a \in \mathbb{Z}$ and $\mathbb{Z}/H = \{H, 1 + H\}$. By the way we have defined μ, $\mu(aH)$ is 1 if a is odd and 0 if a is even.Thus, μ is an isomorphism from $\mathbb{Z} / H$ to $\mathbb{Z}_2$.

b) Similarly, consider the subgroup $5\mathbb{Z}$ which is also a normal subgroup of $\mathbb{Z}$.The cosets of $5\mathbb{Z}$ are $5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$.Therefore, the quotient group $\mathbb{Z} / 5\mathbb{Z}$ is a group with 5 elements. And this factor group is isomorphic to the set $\{0,1,2,3,4\}$ with addition modulo 5; that is, it is sometimes said that $\mathbb{Z} / 5\mathbb{Z}$ equals the set $\{0,1,2,3,4\}$ with addition modulo 5.

Let $\phi(m)$ =remainder of $m \in \mathbb{Z}$ when divided by 5.

Then, by the definition of ϕ, Kernel of ϕ, Ker(ϕ) $= \{m \in \mathbb{Z} : \phi(m) = 0\}$, is the set of all multiples of $5, 5\mathbb{Z}$.

Let H =Ker(ϕ).Then clearly H is a subgroup.

Define $\mu : \mathbb{Z} / H \longrightarrow \mathbb{Z}_5$ as $\mu(aH) = \phi(a)$for $a \in \mathbb{Z}$ and

$$\mathbb{Z}/H = \{ 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

By the way we have defined μ:

$\mu\ (5\mathbb{Z}) = 0, \mu(1 + 5\mathbb{Z}) = 1, \mu(2 + 5\mathbb{Z}) = 2, \mu(3 + 5\mathbb{Z}) = 3and\mu(4 + 5\mathbb{Z}) = 4$.

Thus, μ is an isomorphism from $\mathbb{Z}/H$to $\mathbb{Z}_5$.

c) Generally, consider the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, the set of all multiples of n. Clearly $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, since $\mathbb{Z}$ is an abelian group. The cosets of $n\mathbb{Z}$ are $\{ n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, \dots, (n-2) + n\mathbb{Z}, (n-1) + n\mathbb{Z}\}$.Therefore, the quotient group $\mathbb{Z} / n\mathbb{Z}$ is a group with n elements. And this factor group is isomorphic to the set $\{0,1,2,3,4, \dots, (n-1)\}$ with addition modulo n; that is, it is sometimes said that $\mathbb{Z} / n\mathbb{Z}$ equals the set $\{0,1,2,3,4, \dots, (n-1)\}$ with addition modulo n.

Let $\phi(m)$ =remainder of $m \in \mathbb{Z}$ when divided by n.

Then, by the definition of ϕ, Kernel of ϕ, Ker$(\phi) = \{m \in \mathbb{Z} : \phi(m) = 0\}$, is the set of all multiples of n.

Let H =Ker(ϕ).Then clearly H is a subgroup.

Define $\mu : \mathbb{Z} / H \longrightarrow \mathbb{Z}_n$ as $\mu(aH) = \phi(a)$for $a \in \mathbb{Z}$ and

$\mathbb{Z}/H = \{ n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, \dots, (n-2) + n\mathbb{Z}, (n-1) + n\mathbb{Z}\}$.

By the way we have defined μ:

$\mu\ (n\mathbb{Z}) = 0, \mu(1 + n\mathbb{Z}) = 1, \mu(2 + n\mathbb{Z}) = 2, \mu(3 + n\mathbb{Z}) = 3$,

$\mu(4 + n\mathbb{Z}) = 4$ etc.

Thus, μ is an isomorphism from $\mathbb{Z}/H$ to $\mathbb{Z}_n$.

CHAPTER 3

UNIQUE FACTORIZATION DOMAINS
AND
EUCLIDEAN DOMAINS

$\mathbb{Z}$ $-$UNIQUE FACTORIZATION DOMAIN

The integral domain $\mathbb{Z}$ is our standard example of an integral domain in which there is unique factorization into primes.

DEFINITION

Let R be a commutative ring with unity and let $a, b \in R$. If there exist $c \in R$ such that $b = ac$, then a **divides** b, denoted by $a|b$. We read $a \nmid b$ as " a does not divide b".

DEFINITION

An element u of a commutative ring with unity R is a unit of R if u divides 1, that is, if u has a multiplicative inverse in R.Two elements $a, b \in R$ are **associates** in R if $a = bu$, where u is a unit in R.

ASSOCIATES IN $\mathbb{Z}$

The only units in $\mathbb{Z}$ are1 and -1.Thus two elements $a, b \in \mathbb{Z}$ are associates if $a = (1)b$ or $a = (-1)b$.That is, only associates of $a \in \mathbb{Z}$ are a and $-a$ in $\mathbb{Z}$.

For example, only associates of:

- 26 in $\mathbb{Z}$ are 26 and -26
- 10 in $\mathbb{Z}$ are 10 and -10

DEFINITION

A nonzero element p that is not a unit of an integral domain D is an **irreducible** of D if in every factorization $p = ab$ in D has the property that either a or b is a unit.

Note that an associate of irreducible p is again an irreducible, for if $p = uc$ for a unit u, then any factorization of c provides a factorization of p.

IRREDUCIBLE ELEMENTS IN $\mathbb{Z}$

In $\mathbb{Z}$, the irreducible elements are the integers p and$-p$, where p is a prime number since $p = (1)p$ and $-p = (-1)p$, where 1 and -1 are the only units in $\mathbb{Z}$. The prime elements of $\mathbb{Z}$ are exactly the irreducible elements - the prime numbers and their negatives.

For example,

- 2 and -2 are irreducible in $\mathbb{Z}$ since $2 = (1)2$ and $-2 = (-1)2$, where 1 and -1 are the units in $\mathbb{Z}$
- Similarly, 31 and -31 are irreducible in $\mathbb{Z}$since$31 = (1)31$ and $-31 = (-1)31$, where 1 and -1 are the units in $\mathbb{Z}$
- Generally, p and $-p$ (where p is a prime number) are irreducible in $\mathbb{Z}$ since $p = (1)p$ and $-p = (-1)p$, where 1 and -1 are the units in $\mathbb{Z}$.

DEFINITION

An integral domain D is a **unique factorization domain** (abbreviated UFD) if the following conditions are satisfied:

1. Every element of D that is neither 0 nor a unit can be factored into a product of finite number of irreducibles.
2. If $p_1 \dots p_r$ and $q_1 \dots q_s$ are two factorizations of the same element of D into irreducible, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates.

THEOREM

Every **Principal ideal domain** is a **Unique factorization domain.**

PROOF

If D is a principal ideal domain, then each $a \in D$, where a is neither 0 nor a unit, has a factorization

$$a = p_1 p_2 p_3 \dots p_r$$

into irreducible. It remains for us to show the uniqueness. Let

$$a = q_1 q_2 q_3 \dots q_s$$

be another such factorization into irreducible. Then we have $p_1 | (q_1 q_1 \dots q_s)$, which implies that $p_1 | q_j$ for some j. By changing the order of the q_j if necessary, we can assume that $j = 1$ so $p_1 | q_1$. Then $q_1 = p_1 u_1$, and since $p_1$is an irreducible, u_1 is a unit, so p_1 and q_1 are associates. We have then

$$p_1 p_2 \dots p_r = p_1 u_1 q_2 \dots q_s,$$

So by the cancellation law in D,

$$p_2 \dots p_r = u_1 q_2 q_3 \dots q_s.$$

Continuing this process, starting with p_2 and so on, we finally arrive at

$$1 = u_1 u_2 u_3 \dots u_r q_{r+1} \dots q_s.$$

Since the q_j are irreducible, we must have $r = s$.

FUNDAMENTAL THEOREM OF ARITHMETIC

The integral domain $\mathbb{Z}$ is a **UFD**.

PROOF

We have seen that all ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z} = \langle \mathrm{n} \rangle$, for n $\in$ $\mathbb{Z}$**.** That is, every ideal of $\mathbb{Z}$ is principal ideal and thus $\mathbb{Z}$ is a principal ideal domain. Then by the previous theorem, $\mathbb{Z}$ is a unique factorization domain.

For example, in $\mathbb{Z}$

- Consider the two factorizations of 24,

  $$24 = (2)(2)(3)(2) = (-2)(-3)(2)(2).$$

  Here 2 and -2 are associates, as are 3 and -3. Thus except for the order and associates, the irreducible factors in these two factorizations of 24 are the same.

- Now consider

  $$30 = (2)(3)(5) = (-2)(-3)(5).$$

  Here 2 and -2 are associates, as are 3 and -3. Thus except for the order and associates, the irreducible factors in these two factorizations of 30 are the same.

- Now

  $$148 = (2)(2)(37) = (-2)(2)(-37).$$

  Here 37 and -37 are associates, as are 2 and -2. Thus except for the order and associates, the irreducible factors in these two factorizations of 148 are the same.

EUCLIDEAN DOMAIN

A Euclidean norm on an integral domain D is a function υ from nonzero elements of D into non negative integers such that following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$ there exist $q\ and\ r$ in D such that $a = bq + r$ where either $r = 0$ or $\upsilon(r) < \upsilon(b)$
2. For all $a, b \in D$, where neither a nor b is zero, $\upsilon(a) \leq \upsilon(ab)$

An integral domain D is a **Euclidean domain** if there exist a Euclidean norm on D.

IN CASE OF INTEGERS ℤ:

Integral domain ℤ is a Euclidean domain for the norm function given by $\upsilon(n) = |n|$ for $n \neq 0$ in ℤ.

Condition 1 holds for ℤ by division algoritham,

That is if m is a positive integer and n is any integer, then there exist unique q and r such that $n = mq + r, 0 \leq r < m$.

Condition 2 follows from $|ab| = |a||b|$ and $|a| \geq 1$ for $a \neq 0$ in ℤ.

$1 \leq |a|$

$1 \leq |a||b| (\because |b| \geq 1\ forb \neq 0)$

$1 \leq |ab|$

$|ab| \geq |a|$

$\upsilon(ab) \geq \upsilon(a)$

ARITHEMATIC IN EUCLIDEAN DOMAIN

THEOREM

For a Euclidean domain, with Euclidean norm υ , $\upsilon(1)$ is minimal among all $\upsilon(a)$ for non zero $a \in D$ and $u \in D$ is a unit if and only if $\upsilon(u) = \upsilon(1)$

PROOF

Condition 2 for υ tells us at once that for $a \neq 0$,

$$\upsilon(1) \leq \upsilon(1 \cdot a) = \upsilon(a)$$

On other hand, If u is a unit in D then $\upsilon(u) \leq \upsilon(uu^{-1}) = \upsilon(1)$.Thus $\upsilon(u) = \upsilon(1)$ for a unit u in D.Conversly suppose that a non zero $u \in D$ is such that $\upsilon(u) = \upsilon(1)$ then by the division algorithem there exist q and r in D such that $1 = uq + r$ where either $r = 0$ or $\upsilon(r) < \upsilon(u)$.But since $\upsilon(u) = \upsilon(1)$ is minimal over all $\upsilon(d)$ for non zero $d \in D$,$\upsilon(r) < \upsilon(u)$ is impossible. Hence $r = 0$ and $1 = uq$ so u is a unit.

Example in case of $\mathbb{Z}$

$\upsilon(n) = |n|$is the Euclidean norm for $\mathbb{Z}$ and the minimum of $\upsilon(n)$ for non zero $n \in \mathbb{Z}$ is 1. And 1 and -1 are the only elements of $\mathbb{Z}$ with $\upsilon(n) = 1$.Ofcourse 1 and -1 are exactly the units of $\mathbb{Z}$.

CHAPTER 4

GAUSSIAN INTEGERS

Gaussian Integer is a complex number whose real and imaginary parts are both integers. They form Commutative ring under usual addition and multiplication. The set of Gaussian Integers is denoted by $\mathrm{Z}[i] = \{a + ib \ : a, b \in \mathbb{Z}\}$.

RING OF GAUSSIAN INTEGERS

Clearly $\mathrm{Z}[i]$ is a subset of $\mathbb{C}$. Also $(\mathbf{Z}[\boldsymbol{i}], +, \times)$ is a commutative ring which is a subring of $(\mathbb{C}, +, \times)$.

i. $x, y \in \mathrm{Z}[i]$

$x = a + ib \quad y = c + id$, $a, b, c, d \in \mathbb{Z}$

$x + y = (a + c) + (b + d)i \quad \in \mathrm{Z}[i]$

$\mathrm{Z}[i]$ is closed under usual addition

ii. Since addition of complex numbers is associative,

$$x + (y + z) = (x + y) + z, \forall\, x, y, z \in \mathrm{Z}[i]$$

iii. There exist $0 = 0 + 0i \in \mathrm{Z}[i]$ such that

$$x + 0 = 0 = 0 + x, \forall x \in \mathrm{Z}[i]$$

That is, 0 is the additive identity in $\mathrm{Z}[i]$

iv. For $a + ib \in \mathrm{Z}[i]$, $\exists - a - ib \in \mathrm{Z}[i]$ since $-a, -b \in \mathbb{Z}$, such that

$(a + ib) + (-a - ib) = (0 + 0i) = (-a - ib) + (a + ib)$

Additive inverse exist for every element in $\mathrm{Z}[i]$

v. Since addition of complex numbers is commutative,

$$x + y = y + x, \forall\, x, y \in \mathrm{Z}[i]$$

vi. $x, y \in \mathrm{Z}[i]$

$x = a + ib \quad y = c + id \;, a, b, c, d \in \mathbb{Z}$

$$xy = (a + ib)(c + id) = (ac - bd) + (bc + ad)i \;\in\; \mathrm{Z}[i]$$

That is, $\mathrm{Z}[i]$ is closed under usual multiplication

vii. Since multiplication of complex numbers is associative,

$$x(yz) = (xy)z \;\; \forall x, y, z \;\in \mathrm{Z}[i]$$

viii. Since the multiplication of complex numbers is distributive over addition,

$$x(y + z) = xy + xz$$

$$(x + y)z = xz + yz \;\forall\; x, y, z \;\in\; \mathrm{Z}[i]$$

ix. Since the multiplication of complex numbers is commutative,

$$xy = yx \;\; \forall x, y \;\in \mathrm{Z}[i]$$

∴ $(\mathbf{Z}[\boldsymbol{i}], +, \times)$is a commutative ring

IDEALS OF GAUSSIAN INTEGERS

Let $S = \{a + ib : a, b \in \mathbb{Z}, b \; is \; even\}$.

Clearly $0 \;\in S$. Therefore, S is nonempty.

Let $x, y \in S$. Take $x = a + ib$ and $y = c + id$, where b, d is even.

Then $x - y = (a - c) + i(b - d)$.

Since both b and d are even, $b - d$ is even. This implies that $x - y \;\in\; \mathbb{Z}[i]$.

Furthermore, the product $xy = (ac - bd) + i(bc + ad)$. Again note that bc and ad are even. That is, $xy \;\in \mathbb{Z}[i]$.

This proves that S is a subring of $\mathbb{Z}[i]$.

Now, let $1 + 2i \;\in S$and $i \in \mathbb{Z}[i]$.

Then $i(1 + 2i) = i - 2 \;\notin S$ since 1 is not an even integer.

That is, S is not an ideal of $\mathbb{Z}[i]$.

INTEGRAL DOMAIN OF GAUSSIAN INTEGERS

We know $\mathbf{Z}[\boldsymbol{i}]$ form a commutative ring under addition and multiplication .Also $\mathrm{Z}[i]$ form integral domain under the same operations.

PROOF:

$(\mathrm{Z}[i],+,\times)$is a commutative ring.

Let $x, y \in \mathrm{Z}[i]$ and $x, y \neq 0$

Since $\mathrm{Z}[i] \subset \mathbb{C}$, $x = r_1 e^{i\theta_1}$ and $y = r_2 e^{i\theta_2}$ where $r_1 , r_2 \neq 0$

Then $xy = r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)} \neq 0$ $(\because \; r_1, r_2 \neq 0)$

That is, $\mathrm{Z}[i]$ has no zero divisors in it.

$\therefore$ $\mathrm{Z}[i]$ is an integral domain.

NORM OF A GAUSSIAN INTEGER

For a Gaussian integer $\alpha = a + ib$, norm is $N : \mathrm{Z}[i] \rightarrow \mathbb{Z}$ defined as $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$, where $\overline{\alpha}$ is complex conjugate of α.

- ❖ An element $\alpha \in \mathrm{Z}[i]$ is a unit if and only if $N(\alpha) = \pm 1$.

  PROOF

  Suppose $\alpha \in \mathrm{Z}[i]$ is a unit in ring $\mathrm{Z}[i]$. Then there exist some $\beta \in \mathrm{Z}[i]$ such that $\alpha\beta = 1$

  Then $N(\alpha\beta) = (\alpha\beta)\left(\overline{\alpha\beta}\right)$

  $= (\alpha\bar{\alpha})\left(\beta\bar{\beta}\right)$

  $= N(\alpha)N(\beta)$

  Since $N(1) = 1 \Longrightarrow N(\alpha)N(\beta) = 1$ in ring $\mathbb{Z}$

  Since $N(\alpha)$ and $N(\beta)$ are both integers, it follows that

  $N(\alpha) = N(\beta) = \pm 1$

  Conversely, Suppose that $N(\alpha) = \pm 1$ for some $\alpha \in \mathrm{Z}[i]$

  Then let $\beta = N(\alpha^{-1})\bar{\alpha}$

  Since $N(\alpha) = 1 \Longrightarrow N(\alpha^{-1}) = \pm 1$

  Clearly element $\beta \in \mathrm{Z}[i]$

  Then $\beta\alpha = N(\alpha^{-1})\bar{\alpha}$

  $= N(\alpha^{-1})N(\alpha)$

  $= 1$

Thus α is a unit in $\mathrm{Z}[i]$

- Since the $N(1) = N(-1) = N(i) = N(-i) = 1$, $1, -1, i, -i$ are the units in $\mathrm{Z}[i]$

EUCLIDEAN DOMAINOF GAUSSIAN INTEGERS

Let $a, b \in \mathrm{Z}[i]$with $a \neq 0$and $b \neq 0$.

Then$a = c_1 + id_1$ and $b = c_2 + id_2$ for some integers c_1, c_2, d_1, d_2.

Define norm function as $d(\alpha) = d(a + ib) = a^2 + b^2$

Then $d(a) = c_1^2 + d_1^2$ and $d(b) = c_2^2 + d_2^2$

$ab = (c_1c_2 - d_1d_2) + i(d_1c_2 + d_2c_1)$

$$\begin{aligned} d(ab) &= (c_1c_2 - d_1d_2)^2 + (d_1c_2 + d_2c_1)^2 \\ &= c_1^2c_2^2 + d_1^2d_2^2 + d_1^2c_2^2 + d_2^2c_1^2 \\ &= (c_1^2 + d_1^2)c_2^2 + (c_1^2 + d_1^2)d_2^2 \\ &= (c_1^2 + d_1^2)(c_2^2 + d_2^2) \end{aligned}$$

Since $c_2, d_2 \neq 0 \Longrightarrow c_2^2 + d_2^2 \geq 1$

$\therefore \quad d(ab) \geq c_1^2 + d_1^2 = d(a)$

$d(ab) \geq d(a) \; \forall a, b \in \mathrm{Z}[i]$

$\therefore$ d-function satisfies one of two conditions required for Euclidean domain.

The another thing we need to prove is that, for any $x, y \in \mathrm{Z}[i], \exists q, r \in \mathrm{Z}[i]$ such that $y = qx + r$with $r = 0$ or $d(r) < d(x)$, where $x = a + ib$ and $y = c + id$ with $y \neq 0$.

Let $\frac{y}{x} = \alpha + i\beta, \alpha, \beta \in \mathbb{Q}$. Let q_1, q_2 be two integers in $\mathbb{Z}$ close as possible to rational numbers α and β.

Let $q = q_1 + iq_2$ and $r = y - qx$.

If $r = 0$,then we are done. Otherwise, by the construction of q, we see that $|\alpha - q_1| \leq \frac{1}{2}$ and $|\beta - q_2| \leq \frac{1}{2}$

Therefore, $N\left(\frac{y}{x} - q\right) = N[\alpha + i\beta - (q_1 + iq_2)]$

$$\begin{aligned} &= N[(\alpha - q_1) + i(\beta - q_2)] \\ &\leq (1/2)^2 + (1/2)^2 \\ &= \frac{1}{2} \end{aligned}$$

Thus we obtain,

$$\begin{aligned} N(r) &= N(y-qx) \\ &= N\left[x\left({}^{y}/_{x} - q\right)\right] \\ &= N(x)N\left({}^{y}/_{x} - q\right) \\ &\le \tfrac{1}{2}N(x), \end{aligned}$$

so we do indeed have $N(r) < N(x)$ as we desire.

That is, $Z[i]$ is a Euclidean domain and Euclidean norm is given by $N(\alpha)$ for nonzero $\alpha \in Z[i]$.

CONCLUSION

Abstract algebra has a interesting way of making a problem more transparent by forgetting about superfluous properties. Because of its generality, abstract algebra is used in many fields of mathematics and science.

The integers form the smallest group and the smallest ring containing the natural numbers. The integers are only nontrivial totally ordered abelian group whose positive elements are well ordered. Again in the language of abstract algebra, the set of all integers $\mathbb{Z}$ is a Euclidean domain.This implies that set of all integers is a principal ideal domain and any positive integer can be written as the product of primes in an essentially unique way.

BIBLIOGRAPHY

A First Course In Abstract Algebra-Seventh Edition-John B. Fraleigh

Contemporary Abstract Algebra- Joseph A. Gallian