Ring Theory 3

16 September 2023 17:05

Quadratic Integer Rings:-

Let D be squarefree integer.

$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ is a subring.

$\Rightarrow \mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{Q}(\sqrt{D})$

$\mathbb{Q}(\ ) \rightarrow$ Field

$\mathbb{Q}[\ ] \rightarrow$ Ring

If $D \equiv 1 \pmod 4$ then, $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{D}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$

$= \left\{a + \frac{b}{2} + \frac{b}{2}\sqrt{D} \mid a, b \in \mathbb{Z}\right\}$ is a subring

$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$

If $D \equiv 1 \pmod 4$ then $\omega = \frac{1+\sqrt{D}}{2}$

else $\omega = \sqrt{D}$

If $D = -1$ then we get $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

Polynomial Rings:-

We have R as a ring (often commutative). Polynomials are of the form,

$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ & $a_n \neq 0$

This polynomial is said to be a polynomial ring if $a_i \in R$ which is denoted by $R[x]$

$(a_n x^n + \cdots + a_0)(b_n x^n + \cdots + b_0) = \sum a_i b_j x^{i+j}$, $a_i b_j \in R$ as well

R is the set of constant polynomials in $R[x]$.

If R is commutative then $R[x]$ is also commutative.

R is the constant polynomials . . .

If R is commutative then $R[x]$ is also commutative.

$\mathbb{Z}[x]$ is polynomial ring. polynomial

$\mathbb{Z}/4\mathbb{Z}[x]$ is a commutative ring.

<u>Proposition</u>:— Let R be an integral domain and let $p(x)$ and $q(x)$ be non-zero elements of $R[x]$. Then

(1) degree of $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$

(2) the units of $R[x]$ are just units of R

(3) $R[x]$ is an integral domain

<u>Matrix Rings</u> :—

R is a ring and a $M_n(R)$ is a matrix Ring if all entries in $M_n(R)$ belongs to R and is of dimension $n \times n$

$M_n(R)$ may or may not be commutative even if R is commutative

If $S \subseteq R$ is a subring then $M_n(S) \subseteq M_n(R)$ is also a subring

$M_n(\mathbb{Z}) \subseteq M_n(\mathbb{Q}) \subseteq M_n(\mathbb{R}) \subseteq M_n(\mathbb{C})$

Set of Upper triangular matrices is also a subring of $M_n(R)$

<u>Group Rings</u> :—

$G = \{g_1, g_2, \dots, g_n\}$ be any finite group with operation $\times$

R is a commutative ring with identity $1 \neq 0$

RG is a group ring

Set of all, $a_1g_1 + a_2g_2 + \dots + a_ng_n$ where $a_i \in R$

Set of all, $a_1 g_1 + a_2 g_2 + \cdots + a_n g_n$ where $a_i \in R$

If g_i is identity we may write $a_i g_i$ as a_i

$e(RG) = RG$

RG is commutative iff G is commutative

$e a_1 g_1 + e a_2 g_2 + \cdots + a_n g_n = g_1 + g_2 + \cdots g_n$

Identity of RG is identity of R.

$\Rightarrow (ea_i - g_i) = 0 \Rightarrow e = 1$

$G = D_8$ is a dihedral group of order 8

$\langle r, s \rangle$ $\quad r^4 = 1 \quad s^2 = 1 \quad rs = sr^{-1}$

$R = \mathbb{Z}$

$RG = \mathbb{Z} D_8$ is a group ring.

$r^2 + r + 3rs \in \mathbb{Z} D_8$

$\hookrightarrow r^2 + r + rs + rs + rs \in \mathbb{Z} D_8$

• Domain is a ring with no zero divisors.

Q) A be a ring and ~~A be a domain, i.e., has no zero-divisors.~~ Then if $ab = 1$ for some $a, b \in A$. Prove that $ba = 1$, i.e., a, b are units in A.

Ans:- $ab = 1 \Rightarrow aba = a \Rightarrow aba - a = 0 \Rightarrow a(ba - 1) = 0$

$\Rightarrow ba = 1$

Q) Let A be a ring and $a, b \in A$ such that $ab = 1$. Prove that ba and $1 - ba$ are idempotents in A

Ans:- $(ba)^2 = baba = ba$

$(1 - ba)^2 = (1 - ba)(1 - ba) = 1 - 2ba + (ba)^2 = 1 - 2ba + ba = 1 - ba$

Q) $a, b, c \in A$. A is a ring such that $ab = ca = 1$. Prove that $c = b$ and a is a unit of A.

Ans:— $ab = 1$

$\Rightarrow cab = c = b$. Thus a is a unit

$R = GL_6(\mathbb{Z}_2)$.

↳ non-commutative ring

Ord(R)

$= (2^6-1)(2^6-2)\cdots(2^6-2^5)$

$R = GL_n(R')$ $\quad$ Ord$(R') = m$

nxn matrix with each entry having m choices

$$\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix} \begin{array}{l} \to m^n - 1 \\ \to m^n - m \\ \\ \to m^n - m^{n-1} \end{array}$$

$\text{Ord}(GL_n(R')) = (m^n-1)(m^n-m)\cdots(m^n-m^{n-1})$

Q) Let R be ring and $a, b \in R$ such that $ab = ba$ is a unit of R. Prove that a and b are both units in R.

Ans:— ab is a unit of R $\Rightarrow \exists\, c \in R$ such that $abc = cab = 1$

$a(bc) = cba = (cb)a = 1$ $\quad \Rightarrow a$ is a unit

Similarly b is a unit.