Rings and Modules

B.Sury

Contents

Lectures

- I tried to latex all lecture notes and to make a concise notes, but due to time constraint it's remains undone.

1.1 Lecture-1

- Examples of rings ; X is a **finite** set with powerset $\mathcal{P}(X)$ with $A+B = A\Delta B$, $A.B = A\cap B$ and $A^{-1} = A$. This ring has unity X. X is infinite then, $R = \{\text{all set of finite number of elements}\}$ is also a ring but with no unity.
- $C_c((0,1],\mathbb{R}))$ is the ring of all continuous function from $(0,1]$ to $\mathbb{R}$ with compact support.
- R is a finite ring then $\exists m \neq n$ such that $a^m = a^n$ for all $a \in R$.

  $$P_k : x \mapsto x^k$$

  We can vary k to get different functions. since R is finite R^R has finite cardinality. There is some $m \neq n$ such that $P_m = P_n$.
- A ring might not have unity but a subring can have unity. Example- $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a, b \in R \right\}$ has unity $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.
- Defination of **Charecterestic of a Ring , Integral Domain, Field, Zero divisors**.
- $\mathbb{Z}_n$ is domain iff n is prime.
- R finite integral domain then R is field. (Look ar $a \neq 0$ in R then $\{ar_1, \cdots, ar_k\}$ is R so $ar_i = 1$ for some unique r_i.)
- $M_n(R)$ has zero divisors for any commutative ring R.
- Defination of **nilpotent element, Polynomial ring**.
- Let, $k = \prod p_i^{\alpha_i}$. In $\mathbb{Z}_k$, s is a nilpotent element $\Leftrightarrow$ $p_i \mid s$ forall $i \in \{1, \cdots, r\}$.
- For a ring R , the set of units are defined as R^*. $M_n(\mathbb{Z})$ be the ring $M_n(\mathbb{Z})^* = \{A : \exists B; AB = BA = I\}$. Which is precisely $\{\det(A) = \pm 1\}$.
- Reference *From Numbers to Rings: The Early History of Ring Theory* - Israel Kleiner.

1.2 Lecture-2

- G be a finite group and R be nay commutative ring with unity. Then **Group Ring** is the set of all function from G to R.
$$R[G] = \{\varphi : G \to R\}$$
Here addition is $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$. And multiplication $*$ is defined as,
$$(\varphi * \psi)(g) = \sum_{xy=g} \varphi(x)\psi(y)$$
$R[G]$ is commutative iff G is abelian. If R is a field then $R[G]$ is an **R-Algebra**. For infinite we can define $R[G]$ as $\{\varphi : G \to R \text{ with } |\text{Supp}(\varphi)| < \infty\}$.

- (**Dorroh Extension**) Any ring without unity can be embedded in a ring with unity. Look at $R \times \mathbb{Z}$. $(r, m) \cdot (s, n) = (ms + nr + rs, mn)$ with unity $(0, 1)$.

- $\bar{\mathbb{Z}} = \{\alpha \in \mathbb{C} : \alpha \text{ satisfy a monic Polynomial in } \mathbb{Z}[x]\}$ is **Algebraic integral Ring**. Let, $\alpha, \beta \in \bar{\mathbb{Z}}$ then $\alpha^n \in \sum_{i=0}^{n-1} \mathbb{Z}\alpha^i, \beta^n \in \sum_{i=0}^{m-1} \mathbb{Z}\beta^i$. We will show that $\alpha\beta \in \bar{\mathbb{Z}}$. Now define $A = \sum \mathbb{Z}\alpha^i\beta^j$ here sum is over $0 \le i \le n$ and $0 \le j \le m$. Let, $A = \sum_{i=1}^{d} \mathbb{Z}a_i$. Now we will show that $A \subseteq \bar{\mathbb{Z}}$. if $a \in A$ then,
$$\begin{aligned}
aa_1 &= m_{11}a_1 + \cdots + m_{1d}a_d \\
\Rightarrow (a - m_{11}) + (-m_{12})a_2 + \cdots + (-m_{1d})a_d &= 0 \\
\text{Similarly, } (-m_{21})a_1 + (a - m_{22})a_2 + \cdots + (-m_{2d})a_d &= 0 \\
&\vdots \\
(-m_{d1})a_1 + (-m_{2d}) + \cdots + (a - m_{dd})a_d &= 0 \\
\Rightarrow \underbrace{\begin{pmatrix} a - m_{11} & \cdots & -m_{1d} \\ \vdots & \ddots & \vdots \\ -m_{d1} & \cdots & a - m_{dd} \end{pmatrix}}_{M} \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} &= 0
\end{aligned}$$
Now, $\text{adj}M(M)\vec{a} = 0$ which gives $\det(M)I\vec{a} = 0$. Now $1 \in \{a_1, \cdots, a_d\}$ so, $\det(M) = 0$

- $A = \sum_{i=1}^{d} \mathbb{Z}a_i$ is known as **Cayley - Hamilton Ring**.

-

1.3 Lecture-3

- Defination of **Ideals**.Right Ideals, Left Ideals, Both sided Ideals.

- $I = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\right\}$ is Left-Ideal which is not Right Ideal.

- R be a commutative Ring with 1. Then the Ideals of $M_n(R)$ are precisely $M_n(I)$ where $I \triangleleft R$. For any $J \triangleleft M_n(R)$; we have $(E_{ij}TE_{kl})_{il} = T_{jk}$. Here $T \in M_n(R)$. (See rest)

- Defination of **Simple Ring**

- Fields have only Ideal $\{0\}$. $M_n(K)$ is example of simple Ring for a field K.

- Defination of **Maximal Ideal**.

- Let R be a ring with unity. Let $I \subset R$ be proper Ideal , then $I \subseteq m \subset R$ where m is a maximal Ideal.
- Defination of **Unit,Irreducible element, Prime elements**.
- Ideals equivalent to to an Ideal generated by single element are called **Principal ideal**.
- For a field K all Ideals of $K[x]$ are Principal Ideals. $R = K[x]$ has Ideals of form (f) where $f \in R$. (One Property is used here Polynomial ring over a field is a euclidean domain)
- $I = (x, 2)$ is not principal ideal in $\mathbb{Z}[x]$.
- Maximal Ideals of $K[x]$ are (f) where, f is Irreducible.
- If f is an unit of $k[x]$ then all the coefficient of f is nilpotent except the constant term. constant term is unit. So, f has degree 0 as K is field. So, $K[x]^* = K^*$.
- All Ideals of $\mathbb{C}[x]$ are principal. Irreducible Polynomial of it has degree 1.
- R integral domian with $1 \in R$ is a **Principal Ideal Domain (P.I.D)** iff R is field.
- $\mathbb{C}[x, y] = (\mathbb{C}[x])[y]$ is not P.I.D.
- (Hilbert Nullstellensatz) Maximal Ideals of $\mathbb{C}[X, Y]$ are of form $(X - a, Y - b)$ where $a, b \in \mathbb{C}$.
- (Gaussian integers) $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$. $(5) = 5R \subset (2 + i)$ and $(2) = 2R = (1 + i)(1 + i)$.

§ References

[1] Lectures on Rings and Modules - Joachim Lambek.
[2] Transcendence of α^{β} - The Gelfond-Schneider theorem.
[3] Liouville's Constant and Liouville Number - Transcendence of $\sum_{i=1}^{\infty} \frac{1}{10^{-n!}}$.

1.4 Lecture-4

- I is a left Ideal of R ,$I = R \Leftrightarrow$ there is $x \in R$ such that it has a left inverse.
- If $(x) = R$ then x might not have any left or right inverse. E.g. $R = M_2(\mathbb{R})$ and $x = E_{11}$ then $(x) = (E_{11} + E_{21}E_{11}E_{12}) = R$.
- $\text{Ann}(x) = \{r \in R | rx = 0\}$ (Left Annhilator)
- If I is Left Ideal then left $\text{Ann}(I)$ is two sided Ideal.
- Introduced Ring Homomorphism for commutative Rings.
- R be any ring in which I is two sided Ideal then R/I is a ring with multiplication $(a+I)(b+I) = ab + I$.
- Isomorphism theorem's for Rings.

Problems and Solutions

2.1 Lecture-2

R be a ring with unity. a has right inverse and no left inverse. Show that it has infinite many right inverse.

Solution. Let b be a right-inverse of a. For any $i \geq 0$, we define $b_i = (1 - ba)a^i + b$. Show that if a doesn't have a left-inverse, the b_i are pairwise distinct right-inverses of a.

$1 + xy \in R^* \implies 1 + yx \in R^*$

Solution. Interprete this identity is by generalizing it:

$$(\lambda - ba)^{-1} = \lambda^{-1} + \lambda^{-1} b(\lambda - ab)^{-1} a. \qquad (*)$$

Note that this is both more general than the original formulation (set $\lambda = 1$) and equivalent to it (rescale). Now the geometric series argument makes perfect sense in the ring $R((\lambda^{-1}))$ of formal Laurent power series, where R is the original ring or even the "universal ring" $\mathbb{Z}\langle a, b\rangle$:

$$(\lambda - ba)^{-1} = \lambda^{-1} + \sum_{n\geq 1} \lambda^{-n-1}(ba)^n = \lambda^{-1}(1 + \sum_{n\geq 0} \lambda^{-n-1} b(ab)^n a) = \lambda^{-1}(1 + b(\lambda - ab)^{-1} a).$$

For $\lambda = 1, a = x, b = -y$ we can get our desired result.

$$\mathbb{Q}[\sqrt{d}] \cup \bar{\mathbb{Z}} = \begin{cases} \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right], & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}], & \text{if } d \not\equiv 1 \pmod 4 \end{cases}$$

Proof. An element of Algebraic Integral ring is called **Integral element**. A integral element's(α) irreducible polynomial has integer coefficient $\iff$ $\alpha \in \bar{\mathbb{Z}}$. Notice that, $\sqrt{d}$ is Integral as it satisfy $x^2 - d$.

If $d \equiv 1$ mod 4, then the monic irreducible polynomial of $\left(\frac{\sqrt{d}+1}{2}\right)$ over $\mathbb{Q}$ is $x^2 - x + \frac{(1-d)}{4}$ which is in $\mathbb{Z}[x]$, so $\left[\frac{\sqrt{d}+1}{2}\right]$ is integral. Thus the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ contains the subring $\mathbb{Z}[\sqrt{d}]$, and the subring $\mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right]$ if $d \equiv 1$ mod 4. We will show that there are no other integral elements.

An element $a + b\sqrt{d}$ with rational a and $b \neq 0$ is integral iff its monic irreducible polynomial $x^2 - 2ax + (a^2 - db^2)$ belongs to $\mathbb{Z}[x]$. Therefore, $2a$,$2b$ are integers. If $a = \frac{(2k+1)}{2}$, for $k \in \mathbb{Z}$, then it is easy to see that $a^2 - db^2 \in \mathbb{Z}$ iff $b = \frac{2l+1}{2}$ for some $l \in \mathbb{Z}$, and $(2k+1)^2 - d(2l+1)^2$ is divisible by 4. The latter implies that $d \equiv 1$ mod 4. In turn, if $d \equiv 1$ mod 4 then every element $\frac{2k+1}{2} + \left(\frac{2l+1}{2}\right)\sqrt{d}$ is integral.
Thus, integral elements of $\mathbb{Q}(\sqrt{d})$ are equal to $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1$ mod 4, and $\mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right]$ if $d \equiv 1$ mod 4.