Ring Theory

Lecture 16

02/03/2022

Recall: $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$

s.t (1) $n_i \geq 2 \quad \forall i$

(2) $n_{i+1} \mid n_i \qquad 1 \leq i \leq s-1.$

(3) If $|G| = n$ then $n = n_1 n_2 \cdots n_s$.

This is invariant factor decomp.

If $|G| = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$G \cong A_1 \times \cdots \times A_k.$

$A_i \cong \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$

s.t $|A_i| = p^{\alpha}$, $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t$

and $\beta_1 + \cdots + \beta_t = \alpha.$

Obtaining invariant factor from elementry factor :

Example. Fact: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $\gcd(m,n) = 1$.

Suppose $G \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

want to write invariant factor decomposition.

$p=2$	$p=3$	$p=5$
2	3	25
2	3	5
2	1	1.

$n_1 = 150$, $n_2 = 30$, $n_3 = 2$.

$G \cong \mathbb{Z}_{150} \times \mathbb{Z}_{30} \times \mathbb{Z}_2$.

Remark: Using the uniqueness statement of the fundamental Thm we can determine whether any two direct product of finite cyclic gps are isomorphic?

Example Is $\mathbb{Z}_6 \times \mathbb{Z}_{15} \overset{?}{\cong} \mathbb{Z}_{10} \times \mathbb{Z}_9$.

First we check if both of them are of same order (both are of order 90).

Next investigate whether they have the same elementary divisors.

$\mathbb{Z}_6 \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

$\mathbb{Z}_{10} \times \mathbb{Z}_9 \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9$.

Since both of them have different elementary divisor so they are not isomorphic.

Ring Theory:

(1) $(\mathbb{Z}, +)$ is an abelian gp.

wrt multiplication $\mathbb{Z}$ is closed.

$a \cdot 1 = a \quad \forall\, a \in \mathbb{Z}.$

$(a+b)\cdot c = a\cdot c + b\cdot c.$

$\mathbb{Z}$ is a commutative ring

(2) $(\mathbb{Q}, +)$ is an abelian gp.

$\mathbb{Q}$ is closed wrt multiplication

$a \cdot 1 = a \quad \forall\, a \in \mathbb{Q}.$

$\mathbb{Q}$ is a commutative ring.

(3) $(\mathbb{R}, +)$ abelian gp.

$(\mathbb{R}, \cdot)$ has 1.

$\mathbb{R}$ is a commutative ring.

(4) $M_n(\mathbb{R})$ = set of all $n \times n$ matrices.

$M_n(\mathbb{R})$ wrt matrix addition forms a abelian gp.

$M_n(\mathbb{R})$ is closed wrt matrix multiplication and Id matrix exists.

$M_n(\mathbb{R})$ is not a commutative ring.

(5) $\mathbb{R}[x]$ = all poly in x with coeff in $\mathbb{R}$.

$\mathbb{R}[x]$ is commutative ring.

$(\mathbb{R}[x], +)$ forms an abelian gp.

$(\mathbb{R}[x], \cdot)$ multiplication of poly 1 is identity

(6) $C(\mathbb{R}) = \{ f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ is cont}^{n}_{s} \}$.

$(f+g)(x) = f(x) + g(x)$

$(C(\mathbb{R}), +)$ is an abelian gp.

$(f \cdot g)(x) = f(x) \cdot g(x)$. is closed wrt multiplication and has identity elt 1. $C(\mathbb{R})$ is commutative ring.

Defn: A ring R is a set with two law of compositions called '+' and multiplication '$\cdot$' which satisfies the following conditions

(1) $(R, +)$ is an abelian gp with additive identity '0'

(2) Multiplication is associative

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c. \quad \forall a,b,c \in R.$$

(3) $\exists\ 1 \in R$ s.t $a\cdot 1 = 1\cdot a = a$

$\forall a \in R$, called 'multiplicative identity'.

(4) Distributive law:

$$(a+b)\cdot c = ac + b\cdot c \quad \text{and}$$

$$c\cdot(a+b) = c\cdot a + c\cdot b \quad \forall a,b,c \in R.$$

Moreover, if $a\cdot b = b\cdot a$ $\forall a,b \in R$ then R is called commutative ring.

Let R be any ring then I can define $R[x]$ = all poly with coeffs in R. If R is commutative then $R[x]$ is commutative.

Any field is also a ring.

The zero ring $R = \{0\}$ consists of the single elt 0.

Prop'n. Let R be a ring in which $1 = 0$. Then R is the zero ring.

Pf: Let $a \in R$ be any elt.

$$a = a \cdot 1 = a \cdot 0 = 0$$

$\therefore$ Every elt of R 0 which means R is the zero ring.

Propn. Let R be a ring. Then

(1) $0 \cdot a = a \cdot 0 = 0 \quad \forall\, a \in R$.

(2) $(-a) \cdot b = a \cdot (-b) = -ab$

(3) $(-a) \cdot (-b) = a \cdot b \quad \forall\, a, b \in R$.

(4) $-a = (-1) \cdot a \quad \forall\, a \in R$.

Defn. An elt $0 \neq u \in R$ is called a unit in R if there is some $v \in R$ s.t $uv = vu = 1$. The set of units in R is denoted by $R^\times$.

Example The units in $\mathbb{Z}$ are 1 & -1.

and the units $\mathbb{R}[x]$ are non zero constant polys.

Defn Let R be a ring. A non-zero elt a of R is called a zero divisor if $\exists$ a non-zero elt $b \in R$ s.t

$$ab = 0 \quad \text{or} \quad ba = 0.$$

Observe that a zero divisor can never be a unit. Suppose a is a zero divisor which is also a unit. $\exists\ b \neq 0$ s.t $ab = 0$.

Since a is an unit $\exists\ v$ s.t $va = 1$

$$ab = 0$$

$$(va)b = v \cdot 0 = 0$$

$$\Rightarrow \quad 1 \cdot b = 0$$

$$\Rightarrow \quad b = 0. \quad \text{which is a}$$

contradiction.

Example. $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian gp.

$(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is closed under $\cdot$ and $\bar{1}$ is the multiplicative id

$\mathbb{Z}/n\mathbb{Z}$ is a ring.

Let $R = \mathbb{Z}/6\mathbb{Z}$. Then $\bar{2} \cdot \bar{3} = \bar{0}$.

Hence $\bar{2}$ is a zero divisor.

Defn. A subring of a ring R is a subgp of R which is closed under multiplication and contains 1.

Example. $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$.

Ring Homomorphism :

Let R and S be two rings. Then a map $\phi : R \longrightarrow S$ is called a ring homo if

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

(2) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

(3) $\phi(1_R) = 1_S$. $\forall a, b \in R$

Examples (1) $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

$f(m) = m + n\mathbb{Z}$.

check f is a ring homo.

(2) Consider $f : \mathbb{R}[x] \longrightarrow \mathbb{R}$.

$f\left(\sum a_i x^i\right) = \sum_{i=1}^{n} a_i a^i$

where a is a fixed real number.

Defn. Let $\phi : R \longrightarrow S$ be a ring homo.

Then $\ker \phi = \{a \in R \mid \phi(a) = 0\}$.

If ϕ is 1-1 and onto then we called ϕ to be an isomorphism.

Propn. Let $\phi : R \to S$ be a ring homo.

(1) The image of ϕ is a subring of S.

(2). $\ker \phi$ is not a subring of R unless $\ker \phi = R$. Furthermore, if $\alpha \in \ker \phi$ then $r\alpha$ and $\alpha r \in \ker \phi$ $\forall r \in R$

$\ker \phi$ is a subgp of R.

Let $a, b \in \ker \phi$ then $\phi(ab) = \phi(a)\phi(b)$

$\Rightarrow ab \in \ker \phi$. $= 0 \cdot 0$

$= 0$.

Suppose $1_R \in \ker\phi$ then

$$\left.\begin{aligned}\phi(1_R) &= 0_S \\ \text{But } \phi(1_R) &= 1_S.\end{aligned}\right\} \Rightarrow 0_S = 1_S.$$

$\Rightarrow$ S is the zero ring.

Let $a \in R$. then

$$\phi(a) = \phi(a \cdot 1_R) = \phi(a)\phi(1_R)$$
$$= \phi(a) \cdot 0_S = 0_S.$$

$\therefore$ ϕ is the zero map.

Pf of (2). Let $a \in \ker\phi$, ie $\phi(a)=0$ and let $r \in R$. WTS $ra \in \ker\phi$.

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0$$
$$= 0.$$

$\Rightarrow ra \in \ker\phi$

Defn. Let R be a ring and I be a subset of R. Then I is said to be a left ideal if I is a subgp of $(R,+)$ and I is closed under left multiplication with the ring elts. i.e

$$r.I \subseteq I, \quad \forall r \in R.$$

and I is said to be a right ideal if I is a subgp of R and I is closed under right multiplication i.e $I.r \subseteq I$.
A subset I which is both a left ideal & a right ideal is called an ideal.

Example. $R = \mathbb{Z}$. , $I = 6\mathbb{Z}$.

Let $r \in R$ then $rI \subseteq I$

Hence $6\mathbb{Z}$ is an ideal of R.