Ring Theory

Lecture 21

Obtaining invariant factors from elementry factors :

Suppose elementry divisors of G are given say $2, 3, 2, 25, 3, 2, 5$.

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

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

The invariant factor of G are

$$n_1 = 2 \cdot 3 \cdot 25 ; \quad n_2 = 2 \cdot 3 \cdot 5 , \quad n_3 = 2 .$$

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

Useing the uniqueness statements of the fundamental thm we can use these process to determine wheather any two direct product of finite cyclic gps are isomophic.

Eg Is $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ isomorphic to $\mathbb{Z}_{10} \times \mathbb{Z}_9$.

Consider $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ have elematry divisors are 2, 3, 3, 5 and it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

$\mathbb{Z}_{10} \times \mathbb{Z}_9$ have elementry divisors are 2, 5, 9 and is isomo to $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9$.

They doesn't have the same elementry divisors. Therefore they are not isomorphic.

<u>Ring Theory</u>:

(1) $(\mathbb{Z}, +, \cdot)$ is a ring.

(2) $(\mathbb{Q}, +, \cdot)$ " " "

(3) $(\mathbb{R}, +, \cdot)$. " " "

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

addition of matrices form a gp.

multiplication of matrices. is a ring

(5) $\mathbb{R}[x] :\equiv$ Set of all polys in x with coeff from $\mathbb{R}$.

addition of poly $\rightsquigarrow$ gp.

multiplication poly $\rightsquigarrow$ has identity

is a ring

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

$(f+g)(x) = f(x) + g(x) \rightsquigarrow$ gp.

$(f \cdot g)(x) = f(x) \cdot g(x) \rightsquigarrow$ has identity $f(x) = \underline{1}$

is a ring,

Defn: A ring R is a set with two binary operations addition $(+)$ and multiplication $(\cdot)$ which satisfies the following condⁿs:

(1) $(R, +)$ is an abelian gp with identity denoted by '0'.

(2) Multiplication is associative:

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

optional in [Dummit & Foote]

(3) $\exists\, 1 \in R$ s.t $a\cdot 1 = 1\cdot a = a$ $\forall a\in R$, called multiplicative identity.

(4) Distributive law:

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

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

$$\forall a,b,c\in R.$$

If in addition $ab = ba$ $\forall a,b\in R$ then R is commutative ring.

Example. (1) Any field is a ring.

(2) Let R be a ring

$R[x]$ = Set of all poly s in x with coeffs from R.

Then $R[x]$ is a ring.

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

(3) The zero ring $R = \{0\}$ consists of a single elt 0.

Remark. Let R be a ring in which $1=0$. Then R is the zero ring. Let $a \in R$ be any elt. Then $a = 1 \cdot a = 0 \cdot a = 0$. i.e every elt of R is zero.

<u>Propn</u>: Let R be a ring. Then $\forall a \in R$

(1) $0 \cdot a = a \cdot 0 = 0$

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

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

(4) $-a = (-1) \cdot a$

<u>Remark</u> Here '0' & '1' are symbols which denote the additive identity and multiplicative identity respectively.

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

Example: The units in the ring of integers are 1 & -1.

The units in $\mathbb{R}[x]$ are non-zero constant polynomials.

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring.

The units in $\mathbb{Z}/n\mathbb{Z}$ are $\overline{m}$ s.t $\gcd(m, n) = 1$.