Lecture 31

(31.0) Definitions. - A ring R is a (non-empty) set together with two operations $+, \cdot : R \times R \longrightarrow R$ (addition and multiplication respectively) and two distinct elements $0, 1 \in R$ such that

I. $(R, +, 0) \leftarrow$ is an abelian group. That is,

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

(ii) $0+a = a+0 = a \quad \forall\, a \in R$.

(iii) $\forall\, a \in R$, there exists an element $b \in R$ such that
$$a+b = 0 = b+a$$

(iv) (Abelian group) $a+b = b+a \quad \forall\, a,b \in R$.

II. Multiplication is also an associative operation, and $1 \in R$ is neutral for multiplication:

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

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

[Note: We do not impose $\begin{cases} \text{existence of an inverse } (a^{-1}). \\ \text{commutativity for multiplication } (ab = ba) \end{cases}$].

III. Multiplication distributes over addition.

$$\left.\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{aligned}\right\} \forall\, a,b,c \in R$$

(31.1) Examples of Rings.

(i) $R = \mathbb{R}$ set of real numbers with <u>usual</u> addition and multiplication ; 0 & 1.

(ii) $R = \mathbb{Z}$

(iii) $R = \mathbb{Z}/n\mathbb{Z}$ ($+, \cdot$ = addition and multiplication modulo n)

($n \geq 2$)

(iv) $R = M_{2\times 2}(\mathbb{C})$ = set of 2×2 matrices with <u>entries from $\mathbb{C}$</u>. (complex numbers).

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}$$

$$0_R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad ; \quad 1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(v) $R = \mathbb{Z}[X]$ polynomial ring in <u>one</u> variable with coefficients from $\mathbb{Z}$.

Ψ

$f = a_0 + a_1X + a_2X^2 + \dots + a_NX^N$ "typical element of R"

where $N \geq 0$ - called degree of the polynomial f, (assuming, of course, $a_N \neq 0$.)

Addition of polynomials is "component-wise", e.g.

$$(1 + 2X + 3X^9) + (2 + 7X^3 + X^9)$$
$$= 3 + 2X + 7X^3 + 4X^9$$

Multiplication of polynomials is carried out using distributivity, e.g.

$$(1+3X)\cdot(1+5X^2+X^3)$$
$$= 1\cdot(1+5X^2+X^3) + 3\cdot X\cdot(1+5X^2+X^3)$$
$$= 1+5X^2+X^3+3X+15X^3+3X^4$$
$$= 1+3X+5X^2+16X^3+3X^4$$

In symbols:

$$(a_0+a_1X+\dots+a_NX^N)(b_0+b_1X+\dots+b_MX^M)$$
$$= a_0b_0 + (a_1b_0+a_0b_1)X + \dots + (a_\ell b_0 + a_{\ell-1}b_1 + \dots + a_0 b_\ell)X^\ell$$
$$+ \dots + a_N b_M X^{N+M}$$

(vi) $\mathbb{Z}[\sqrt{-1}] \ni a+b.i$ where $a,b \in \mathbb{Z}$.

Multiplication. $(a+bi)(c+di) = ac-bd+(ad+bc)i$

Addition. $(a+bi)+(c+di) = (a+c)+(b+d)i$

It is a <u>quotient</u> of $\mathbb{Z}[X]$ (i.e. we have same structure as that on $\mathbb{Z}[X]$, <u>and</u> an additional rule saying $X^2=-1$.)

(31.2) Some remarks on the examples.

- (iv), (v) and (vi) - are quite general ways of building new rings from old ones:

R : ring ; $n \in \mathbb{Z}_{\geq 1}$ $\rightsquigarrow$ $M_{n\times n}(R)$ is another ring.

R : ring $\rightsquigarrow$ $R[X]$ polynomial ring in one variable with coefficients from R

(e.g. $R = \mathbb{Z}[X]$ $\rightsquigarrow$ $\mathbb{Z}[X_1, X_2, \ldots, X_n]$: polynomial ring in n variables with coefficients from $\mathbb{Z}$)

- (i) : fields are special kind of rings.
- (iii) & (vi) : "quotient rings" - later!

(31.3) Some elementary facts and terminology.

Let R be a ring. For any $a \in R$ we have

$$\boxed{a\cdot 0 = 0\cdot a = 0}$$

because $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$ mult. distributes over addition.

$$\Rightarrow \quad a\cdot 0 = 0$$

An element $a \in R$ is said to be <u>invertible</u> (multiplicatively, of course) if we have $b \in R$ such that $a\cdot b = 1 = b\cdot a$

$R^\times$:= set of invertible elements of R.

Then $R^\times$ is again a group (not necessarily abelian) under multiplication borrowed from R. [easy exercise!].

e.g. (i) $(\mathbb{R})^\times = \mathbb{R} \setminus \{0\}$ every non-zero element has an inverse.

(ii) $(\mathbb{Z})^\times = \{\pm 1\}$.

(iii) $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \left\{ x \in \{1, 2, \dots, n-1\} \text{ such that } \gcd(x, n) = 1 \right\}$

(iv) $\left(M_{2\times 2}(\mathbb{C})\right)^\times = GL_2(\mathbb{C})$

(31.4) Another example. Let H be an abelian group.

R = set of all group homomorphisms $H \xrightarrow{f} H$

Addition : $(f_1 + f_2)(h) = f_1(h) + f_2(h)$

$(\forall\ \underline{f_1, f_2 \in R\ ;\ h \in H}.)$

Multiplication = composition

$(f_1 \cdot f_2)(h) = f_1(f_2(h))$

Notation : $R = \mathrm{End}_{gp}(H)$ "endomorphisms of H"

$$\mathrm{End}_{gp}(H)^{\times} = \mathrm{Aut}_{gp}(H) \quad \text{automorphisms of } H.$$

(31.5) Again let R be a ring. We say

- R is <u>commutative</u> if $a \cdot b = b \cdot a$ $\forall a, b \in R$.

- An element $a \in R$ is said to be a <u>zero-divisor</u> if we can find a non-zero element $b \in R \setminus \{0\}$ such that

$$b \cdot a = 0$$

(eg. $\bar{2} \in \mathbb{Z}/6\mathbb{Z}$ is a zero-divisor.)

- A <u>commutative ring</u> R is said to be an <u>integral domain</u> if $0 \in R$ is <u>the only</u> zero-divisor.

Meaning : in <u>an integral domain R</u>,

$a \cdot b = 0$ and $a \neq 0$ implies $b = 0$.

(eg. $\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Q}$, $\mathbb{R}$ - integral domains.

$\mathbb{Z}/n\mathbb{Z}$ is not an integral domain, if n is not prime.)