Lec 10/15

Monday, October 15, 2018 11:32

Today : Rings

Algebraic Geometry

Algebraic # Theory

Definition: A ring R is a set w/ two binary operations $+$ and $\cdot$ and two distinguished elements 0_R and 1_R s.t.

I. $(R, +)$ is an abelian group with identity 0_R.

II. Multiplication is associative & 1_R is neutral.

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

A ring with only one element = zero ring.

eg $R=\mathbb{Z}$. This is a commutative ring.

$R =$ any field is also a commutative ring.

eg $R = \mathbb{Z}/n\mathbb{Z}$ is another commutative ring.

in $\mathbb{Z}/6\mathbb{Z}$, $2\cdot 3 = 0$

eg $R = M_{2\times 2}(\mathbb{Z})$ is a non-commutative ring.

with zero divisors: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

this axiom works w/ non-commutative rings. i.e. $M_{2\times 2}(\mathbb{R})$.

↓ this even works w/ non-commutative rings. i.e. $M_{2\times 2}(\mathbb{R})$.

$\swarrow$ $\mathbb{Z}$ could be replaced by any ring.

eg Polynomial Ring $R = \mathbb{Z}[X]$ = "polynomials in one variable w/ coefficients in $\mathbb{Z}$".

$\rotatebox{90}{$\in$}$

$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \qquad (a_0, a_1, \ldots, a_n \in \mathbb{Z})$

eg $R = \mathbb{Z}[i]$ Gaussian Integers.

quotient rings: $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ (all commutative rings)

eg R = set of gp homomorphisms $H \longrightarrow H$ of an abelian group H.

$f_1, f_2 : H \longrightarrow H$

$f_1 + f_2 = (\lambda x. (f_1(x) + f_2(x)))$

Ex. this is a ring

$f_1 \cdot f_2 = f_1 \circ f_2$

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

Ex. $\mathrm{End}_{gp}(\mathbb{Z}^2) = M_{2\times 2}(\mathbb{Z})$

$\underbrace{\text{Invertible elements of } R}_{R^\times}$: $a \in R$ s.t. $\exists b$ s.t. $ab = ba = 1_R$.

eg $(\mathbb{Z}/n\mathbb{Z})^\times = x \in \{1, \ldots, n-1\}$ s.t. $(x, n) = 1$.

$$(\mathrm{End}_{gp}(H))^\times = \mathrm{Aut}_{gp}(H)$$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$; same for $\mathbb{C}$. $\mathbb{Z}^\times = \{\pm 1\}$.

We say a ring R is commutative if $\cdot$ is commutative.

$a \in R$ is a zero divisor if $\exists\, b \in R \setminus \{0\}$ s.t. $ab = 0$.

an integral domain is a commutative ring with no zero divisors. (other than 0_R)

not fields

R	
$\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ $\mathbb{Z}[x]$	Integral domain
$\mathbb{Z}/n\mathbb{Z}$ n not prime $M_{n\times n}[F]$	not integral domain

A <u>field</u> is an integral domain where every non-zero element is invertible.

(<u>Lemma</u> if $a \in R^\times$ then a is not a zero divisor

<u>Pf</u> $ab = 1_R$; if $\exists\, c$ s.t. $ac = 0$ then $c = c1_R = cab = 0 \cdot b = 0$.)