Lecture 28

Monday, March 16, 2015 9:59 AM

Rings

Defn A ring $(R, +, \cdot)$ is a set R and 2 binary ops $+, \cdot$ s.t.

① $(R, +)$ is an abelian group

② $\cdot$ is associative

③ $\cdot$ distributes over $+$: $\forall a, b, c \in R$,

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

The ring R is commutative if $\cdot$ is commutative:

$$a \cdot b = b \cdot a \quad \forall a, b \in R$$

The ring R has an identity (or is a ring with 1) if $\exists 1 \in R$ s.t. $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.

A division ring is a ring with $1 \neq 0$ where every $a \in R \setminus \{0\}$ has a multiplicative inverse. A commutative division ring is called a field.

e.g. $\cdot$ $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ are rings (comm w/ 1)

$\cdot$ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ (p prime) are fields

$\cdot$ If $(R, +)$ is an abelian gp, we can define a ring str on it via

$$a \cdot b = 0 \quad \forall a, b \in R$$

This is the trivial ring on $(R, +)$.

- $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$
  is the Hamilton quaternions is a division ring w/ coordinatewise addition and mult'n defined so that Q_8 mult'n happens and distributivity holds.

$$(1+j)\cdot(3+2i-5k)$$
$$= 3+2i-5k+3j-2k-5i$$
$$= 3-3i+3j-7k.$$

- A a ring, X a set. $Map(X, A) = \{ \text{fns } f: X \to A \}$. For $f, g \in Map(X, A)$,

$$f+g : X \longrightarrow A, \quad x \longmapsto f(x)+g(x)$$
$$f\cdot g : X \longrightarrow A, \quad x \longmapsto f(x)\cdot g(x)$$

This is a ring. Comm if A is comm
w/ 1 if A has 1.

- $\mathrm{Map}_c(\mathbb{R},\mathbb{R}) = \{ f:\mathbb{R}\to\mathbb{R} \mid f \text{ has compact support} \}$

  meaning $\exists K \subseteq \mathbb{R}$ $\underbrace{\text{compact}}$ s.t. $f(\mathbb{R}\setminus K) = \{0\}$.

  · closed & bounded

  is a ring w/out 1.

<u>Prop</u> R a ring. Then

1. $0\cdot a = a\cdot 0 = 0 \quad \forall a \in R$
2. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b) \quad \forall a,b\in R$
3. $(-a)\cdot(-b) = ab$
4. If $1\in R$, then 1 is unique & $-a = (-1)\cdot a$. $\square$

<u>Defn</u> A <u>subring</u> $S \subseteq R$ is a subgp $(S,+)$ of $(R,+)$ which is closed under $\cdot$.

<u>e.g.</u> $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ is a chain of subrings.

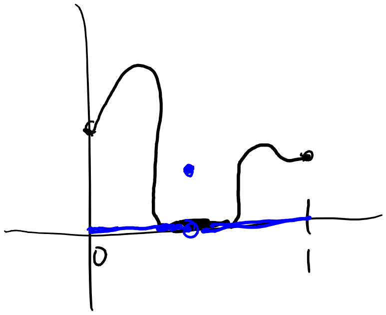
Def'n Let R be a ring.

(1) An element $a \in R \setminus \{0\}$ is a *zero divisor* if $\exists\, 0 \neq b \in R$ s.t. $a \cdot b = 0$ or $b \cdot a = 0$.

(2) Assume $0 \neq 1 \in R$. Then $u \in R$ is called a *unit* of R if $\exists\, v \in R$ s.t. $u \cdot v = v \cdot u = 1$.

Let $R^{\times} = \{ u \in R \mid u \text{ a unit} \}$.

Ring	Zero-divisors	Units
$\mathbb{Z}$	$\emptyset$	$\{\pm 1\}$
$\mathbb{Z}/n\mathbb{Z}$	$\{\bar{a} = a + n\mathbb{Z}$ s.t. $(a,n) \neq 1\}$	$\{\bar{a}$ s.t. $(a,n) = 1\}$
F field	$\emptyset$	$F \setminus \{0\} = F^{\times}$
$\mathcal{F} = \mathrm{Map}([0,1], \mathbb{R})$	$\mathcal{F} \setminus \left(\text{fns which are never } = 0 \cup \{0\} \right)$	$\{ f : [0,1] \to \mathbb{R} \setminus \{0\} \}$



Note If R is a ring w/ 1, then $R^{\times}$ is a group under $\cdot$.

e.g. $Q_8 \leq \mathbb{H}^{\times}$.

Def'n A commutative ring w/ $1 \neq 0$ and no zero divisors is called an integral domain.

e.g. $\mathbb{Z}$, fields, ...

Prop Assume $a, b, c \in R$ a ring and a is not a zero divisor. If $a \cdot b = a \cdot c$, then $a = 0$ or $b = c$. In particular, we have cancellation in an integral domain.

Pf If $ab = ac$, then $ab - ac = 0$

$$a(b-c) = 0$$

since a is not a zero divisor, we must have $b - c = 0 \Rightarrow b = c$. $\square$

Cor Any finite integral domain R is a field.

Pf For $a \in R \setminus \{0\}$, $x \longmapsto ax$ is an injective fn $R \to R$ by cancellation ($ax = ay \Rightarrow x = y$). Thus the fn is a bijection so $\exists\, b \in R \setminus \{0\}$ s.t. $ab = 1$ $\Rightarrow b = a^{-1}$. $\square$

E.g. (1) Polynomial rings:

R comm ring w/ id. Indeterminate x,

$$R[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \mid n \geq 0, a_n \in R \}$$

the polynomial ring in x w/ coeffs in R.

(2) Matrix rings: ring R, $n \in \mathbb{Z}^+$

$$M_n(R) = \{ n \times n \text{ matrices w/ entries in } R \}$$

(3) Group rings: G a gp, R comm ring w/ 1,

$$RG = \{ \sum_{g \in G} a_g g \mid a_g \in R \}$$

$$(g + g') \cdot (h + h') = (gh) + (gh') + (g'h) + (g'h')$$

$g, g', h, h' \in G$

...