31/10

Ring of quaternions

$\mathbb{R}$: set of real numbers

$H(\mathbb{R}) = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,$
$ij = k,\ jk = i,\ ki = j \}$

$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)$

$= (a_1 + a_2) + (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2) k$

$0 \in H(\mathbb{R})$ and $(H(\mathbb{R}), +)$ is an Abelian group

$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)$

$= a_1 (a_2 + b_2 i + c_2 j + d_2 k) + b_1 i (a_2 + b_2 i + c_2 j + d_2 k) + \dots$

Multiplication is defined as

$(b_1 i) \cdot a_2 = (b_1 a_2) i$

$(b_1 i)(c_2 j) = (b_1 c_2)(ij)$

$= (b_1 c_2) k$

Suppose $a + bi + cj + dk \neq 0$

$\Leftrightarrow (a, b, c, d) \neq (0, 0, 0, 0)$

Given $\alpha \in H(\mathbb{R})$, $\alpha = a + bi + cj + dk$, we define

$\bar{\alpha} = a - bi - cj - dk$

$\alpha\bar{\alpha} = (a + bi + cj + dk)(a - bi - cj - dk)$

$$= \begin{matrix} a^2 - abi - acj - adk \\ bai + b^2 - bck + bdj \\ caj + cbk + c^2 - cdi \\ dak - dbj + dci + d^2 \end{matrix} = a^2 + b^2 + c^2 + d^2$$

$\alpha\bar{\alpha} \neq 0$

$\Rightarrow \alpha \cdot \dfrac{\bar{\alpha}}{a^2+b^2+c^2+d^2} = 1$ (So, $H(\mathbb{R})$ is a division ring)

Ring of Functions

Let X be a non-empty set

$\mathcal{F}(X) = \{ f : X \to \mathbb{R} \mid f \text{ is a function} \}$

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

$(fg)(x) = f(x) \cdot g(x)$

$0(x) = 0 \quad \forall x \in X \quad \leftarrow$ zero function [Identity]

$(-f)(x) = -f(x) \quad \forall x \in X \quad \leftarrow$ Inverse

Associative, abelian $(+)$, distributive follow from $\mathbb{R}$

$1(x) = 1 \quad \forall x \in X \quad \leftarrow$ Multiplicative identity

Now, instead of $\mathbb{R}$, we can replace it with R, and all the properties will still hold!

- If R is not commutative, then $\mathcal{F}(X)$ is not commutative

  Because if $ab \neq ba$ in R, we can take $f(x) = a \quad \forall x \in X$ and $g(x) = b \quad \forall x \in X$

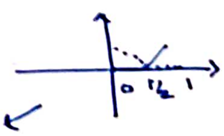
- $X = (0,1)$

  $\mathcal{C}(0,1) = \{ f : (0,1) \to \mathbb{R} \mid f \text{ is continuous} \}$

  We see that $\mathcal{C}(0,1) \subseteq \mathcal{F}((0,1))$

  $f+g$ is continuous

  $f \cdot g$ is continuous



$\Rightarrow \mathcal{C}(0,1)$ is not an integral domain

Definition

* Let $S \subseteq R$ where R is a ring

  Then S is called a subring of R if S is a ring

$\Leftrightarrow$ Equivalent

i) $S \neq \emptyset$

ii) $a, b \in S \Rightarrow a + b \in S$

iii) $a \in S \Rightarrow -a \in S$

iv) $ab \in S$

[Rest all follow from nature of ring R]

Ring of Formal Power Series

$$\mathbb{R}[[x]] = \{ a_0 + a_1 x + a_2 x^2 + \dots \mid a_i \in \mathbb{R} \}$$

$$(a_0 + a_1 x + \dots) + (b_0 + b_1 x + \dots) = (a_0 + b_0) + (a_1 + b_1) x + \dots$$

$$(a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots) = \sum_i c_i x^i$$

$c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$$\Rightarrow c_i = \sum_{\substack{i+j=k \\ i,j \geq 0}} (a_j b_k) x^i$$

(Exercise)

Check that $\mathbb{R}[[x]]$ is a commutative ring with identity, and an integral domain

* For a power series $f(x) = \sum a_i x^i$, we define $\text{ord}(f) = \min \{ i \mid a_i \neq 0 \}$

Quadratic extension fields

Let d be a positive integer, that is not a square

$$\mathbb{Q}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Q} \}$$

$$(a + b\sqrt{d}) + (x + y\sqrt{d}) = (a + x) + (b + y)\sqrt{d}$$

$$(a + b\sqrt{d})(x + y\sqrt{d}) = (ax + byd) + (bx + ay)\sqrt{d}$$

- $\mathbb{Q}[\sqrt{d}] \neq \emptyset$
- Addition is a closed operation
- Inverse exists
- Multiplication is closed

• If $\alpha = a + b\sqrt{d}$, $\bar{\alpha} = a - b\sqrt{d}$

$\alpha\bar{\alpha} = a^2 - db^2$

If $a^2 - db^2 = 0$ and $\alpha \neq 0$

$\Rightarrow d = \frac{a^2}{b^2}$ $(\Rightarrow\Leftarrow)$

$\Rightarrow \alpha\bar{\alpha} \neq 0$

$\Rightarrow \alpha\left(\frac{\bar{\alpha}}{a^2 - db^2}\right) = 1$

Ring homomorphism

From now on, we will consider rings with identity. (R with 1)

Definition

Let R, S be rings. A function $f : R \to S$ is called a ring homomorphism if

① $f(x+y) = f(x) + f(y)$

② $f(xy) = f(x) f(y)$

③ $f(1) = 1$ $[f(1_R) = 1_S]$

A ring homomorphism $f : R \to S$ is said to be an isomorphism if f is a bijection.

(Exercise)

(i) Let $f : R \to S$ be a ring homomorphism. Then

f is an isomorphism $\Leftrightarrow$ $\exists g : S \to R$ a ring homomorphism such that $g \circ f = id_R$ and $f \circ g = id_S$

(ii) $id_R : R \to R$, $r \mapsto r$ is a ring homomorphism

Definition

- Let $f: R \to S$ be a ring homomorphism.

For $s \in S$, the fiber of f over s, denoted by $f^{-1}(s)$, is given by

$$f^{-1}(s) = \{ r \in R \mid f(r) = s \}$$

- Kernel of f, denoted by $\ker f$ is defined to be $\ker f = f^{-1}(0_S) = \{ r \in \mathbb{R} \mid f(r) = 0 \}$

Exercise

Show that

i) $\ker f \neq \phi$

ii) $r_1, r_2 \in \ker f \Rightarrow r_1 + r_2 \in \ker f$

iii) $r \in \ker f$, $a \in R \Rightarrow ar \in \ker f$

- $0_R \in \ker f$
- $f(x+y) = f(x) + f(y)$
- $f(ar) = f(a) f(r) = 0$

- Let R be a ring

A non-empty subset I of R is called a left ideal if

(i) $a, b \in I \Rightarrow a, b \in I$

(ii) $a \in I$, $r \in R \Rightarrow ra \in I$

- In a commutative ring however, $ra = ar$, which make left ideal and right ideal, the same.

Example

1. Let $\mathbb{R}[x]$ be the ring of polynomials with coefficients in $\mathbb{R}$ and $b \in \mathbb{R}$

   I fixed!

   Define $ev_b : \mathbb{R}[x] \to \mathbb{R}$

$$g(x) \to g(b)$$

ev_b is a homomorphism of rings!

Q) What is $\ker(ev_b)$?

$$\ker(ev_b) = \{ f(x) \in \mathbb{R}[x] \mid f(b) = 0 \}$$

$$= \{ (x-b)\, g(x) \mid g(x) \in \mathbb{R}[x] \} \quad (??)$$

follows from degree argument