# Subrings

A subring $S$ of a ring $R$ is a subset $S \subseteq R$ s.t. $S$ is also a ring with operations on $R$

**Prop)** Let $R$ be a ring, $S$ a subset of $R$. Then $S$ is a subring of $R$ if and only if the following are true,

1) $S \neq \emptyset$

2) $rs \in S \quad \forall\, r, s \in S$

3) $r - s \in S \quad \forall\, r, s \in S$

**Ex)** $R = 2\times 2$ real matrices

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{R} \right\} \text{ is a subring}$$

- non-empty
- $A \cdot B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \hat{a} & \hat{b} \\ 0 & \hat{c} \end{pmatrix} = \begin{pmatrix} a\hat{a} & a\hat{b} + b\hat{c} \\ 0 & c\hat{c} \end{pmatrix}$
- $A - B \in T \quad \forall\, A, B \in T$

commutative division ring

## More on Int. Domains and Fields

commutative ring with <u>no</u> zero divisors

**Ex)** Gaussian integers

$$\mathbb{Z}[i] = \{ m + ni \mid m, n \in \mathbb{Z} \}$$

This is a ring, also an integral Domain [check]

$$(a+bi)(c+di) = 0$$

$$(ac-bd) + (bc+ad)i = 0$$

$$\Rightarrow \quad ac = bd \quad \text{and} \quad bc = -ad$$

$$abc = b^2 d \quad \text{and} \quad abc = -a^2 d$$

$$\Rightarrow \quad -a^2 d = b^2 d$$

this is not possible

$$\Rightarrow \quad d = 0 \quad \text{or} \quad -a^2 = b^2$$

or $a = b = 0$

$$\therefore \quad d = 0$$

with some checking $\Rightarrow$ Either $a=b=0$ or $c=d=0$.

$\therefore$ $\mathbb{Z}[i]$ is an integral Domain

Show $\mathbb{Z}[i]$ is not a field (and find the units)

complex conjugent

$$\left[\ \bar{z} = \overline{a+ib} = a - ib\ \right]$$

If $\alpha\beta = 1$ (Since $\bar{1} = 1$)

$$\Rightarrow \quad \overline{\alpha\beta} = \alpha\beta$$

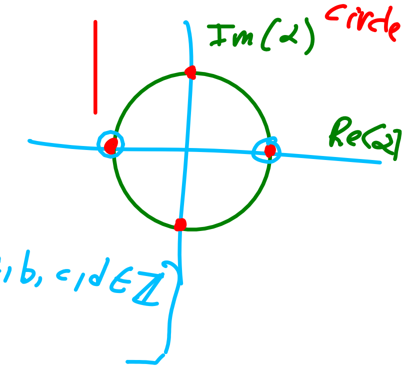
$$\overline{\alpha\beta} = \bar{\alpha}\bar{\beta} = \alpha\beta = 1$$

$$[\alpha = a+ib, \quad \beta = c+id]$$

$$1 = \alpha\beta\bar{\alpha}\bar{\beta} = (a+ib)(c+id)(a-ib)(c-id)$$

$$= (a^2+b^2)(c^2+d^2)$$

only integers on circle




$$\Rightarrow \quad a^2+b^2 = \pm 1 = c^2+d^2$$

$$\Downarrow$$

$$|\alpha| = 1$$

[Remember $a,b,c,d \in \mathbb{Z}$]

$\therefore$ $a^2+b^2 = 1 = c^2+d^2$, Since $a,b,c,d \in \mathbb{R}$

Since $a,b,c,d \in \mathbb{Z}$

$\Rightarrow$ either $a+ib = \pm 1$ or $a+ib = \pm i$

i.e $\alpha = \pm 1$ or $\pm i$ and $\beta = \pm 1$ or $\pm i$

$\therefore$ The only units in $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$

**Prop 1** (cancelation Law)

Let $D$ be a commutative ring, $1 \in D$. Then $D$ is an integral domain iff $\forall a \in D, a \neq 0$, whenever $ab = ac \Rightarrow b = c$.

**Proof:** First suppose $D$ is an integral domain. $a \neq 0$ and let $ab = ac$ $(b, c \in D)$

$$ab - ac = 0$$

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

$\therefore$ Since $a \neq 0$ and $D$ is an int. domain

$$b - c = 0 \Rightarrow b = c.$$

Suppose cancelation holds in $D$

Let $ab = 0$ (say $a \neq 0$)

Know $a0 = 0$

So $ab = a0$, by cancelation

$\Rightarrow b = 0$ $\therefore$ $D$ is an int domain.

∎

Thm: Every finite integral domain is a field.

Proof: Let $D$ be a finite domain

$D^* =$ non-zero elements in $D$

Define a map $\lambda_a : D^* \longrightarrow D^*$ for each $a \in D^*$

$d \longmapsto da$

note $da \in D^*$ since $D$ is an int. domain

$\lambda_a$ is 1-1: if $\lambda_a(d_1) = \lambda_a(d_2)$

$\Rightarrow a d_1 = a d_2 \Rightarrow d_1 = d_2$ by cancelation

$\therefore$ 1-1

$\lambda_a$ is onto since $D^*$ is a finite set and $\lambda_a$ is 1-1

$\therefore \exists\, d \in D^*$ s.t. $\lambda_a(d) = a d = 1$

$\therefore$ d is a left inverse of a, but D is comutitive $\therefore$

$ad = da = 1 \quad \therefore a^{-1} = d$

$\therefore$ D is a field. ∎

Def: Let $n \geq 0$ $n \in \mathbb{Z}$, $r \in R$ a ring

write $nr = \underbrace{r + \cdots + r}_{n \text{ times}}$

Just a notation

The Charcteristic of R is

$\text{Char}(R) =$ least positive $n \in \mathbb{Z}$ s.t. $nr = 0\ \forall r \in R$

$= \text{least positive } n \in \mathbb{Z} \text{ s.t. } \underbrace{r + \cdots + r}_{n \text{ times}} = 0 \quad \forall r \in R$

$= 0$ if no such $n$ exists

Ex) $\text{Char}(\mathbb{Z}_p) = p$ for $p$ prime

Since for $a \in \mathbb{Z}_p$ $\underbrace{a + \cdots + a}_{p \text{ times}} = pa = 0$

$\text{Char}(\mathbb{R}) = \text{Char}(\mathbb{C}) = \text{char}(\mathbb{Q}) = 0$

Lemma/ Let $R$ be a ring, $1 \in R$. If $|1| = n$ (add order)
then $\text{Char}(R) = n$. If $\underset{\underset{1+\cdots+1}{\parallel}}{n1} \neq 0$ $\forall n \neq 0$ $\text{char}(R) = 0$

Proof: Say $n < \infty$, $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$

Fix $r \in R$ $\quad nr = n(1r) = (n1)r = (\overbrace{1 + \cdots + 1}^{=0})r = 0r = 0$

If $n = \infty \implies \underbrace{1 + \cdots + 1}_{n \text{ times}} \neq 0 \quad \forall n$

$\therefore \text{Char}(R) = 0$ ∎

**Theorem:** The characteristic of an integral domain is either zero or prime.

**Proof:**

Let $D$ be int. domain, $Char(D) = n \neq 0$

If $n$ is not prime $\Rightarrow$ $n = ab$, $1 < a < n$, $1 < b < n$

Since $char(D) = n$, then $n \cdot 1 = 0$

$$\Rightarrow (ab) \cdot 1 = 0$$

check

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

$\Rightarrow$ either $a \cdot 1 = 0$ or $b \cdot 1 = 0$

$\Rightarrow$ Either $char(D) = a$ or $char(D) = b$

This is a contradiction of $Char(D) = n > a, b$

$\Rightarrow$ either $n$ is prime or $0$ ∎