Subrings

A subring $S$ of a ring $R$ is a subset $S \subseteq R$ such that $S$ 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) $rs \in S \land r,s \in S$
3) $r-s \in S \land r,s \in S$

Ex. $R = 2 \times 2$ real matrices

$T = \{ (\begin{pmatrix} a & b \\ c & d \end{pmatrix}) \mid a,b,c,d \in \mathbb{R} \}$ is a subring.

- Non-empty
- $A \cdot B = (\begin{pmatrix} a & b \\ c & d \end{pmatrix})(\begin{pmatrix} e & f \\ g & h \end{pmatrix}) = (\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix})$
- $A-B \in T \land a,b \in T$

More on integral domains and fields

\text{commutative ring with no zero divisors}

Ex. $\mathbb{Z}[i] = \{ m+ni \mid m,n \in \mathbb{Z} \}$
This is a ring, also an integral domain [check]

\[(a + bi)(c + di) = 0\]

\[(ac - bd) + (bc + ad)i = 0\]

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

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

\[\Rightarrow -a^2d = b^2d\]

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

\[\therefore d = 0\]

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

\[\therefore \mathbb{Z}[i] \text{ is an integral domain}\]

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

\[z = \frac{1}{a + ib} = a - ib\]

If \(zB = 1\) \((\text{since } T = 1)\)

\[\Rightarrow \overline{z}B = \bar{a} \bar{b}\]

\[\Rightarrow z\overline{z} = a\overline{b} = 1\]

\[1 = a\overline{b} \overline{z} = (a + ib)(c + id)(a - ib)(c - id)\]

\[= (a^2 + b^2)(c^2 + d^2)\]

\[\Rightarrow a^2 + b^2 = \pm 1 = c^2 + d^2\]

\[\therefore a^2 + b^2 = |z|^2 = c^2 + d^2\]

Remember \(a, b, c, d \in \mathbb{R}\)

\[\therefore a^2 + b^2 = |z|^2 = c^2 + d^2\]

Since \(a, b, c, d \in \mathbb{R}\)

\[\therefore \quad \text{either} \quad a + ib = \pm 1 \quad \text{or} \quad a + ib = \pm i\]

\[\therefore z = \pm 1 \text{ or } \pm i \quad \text{and} \quad \overline{z} = \pm 1 \text{ or } \pm i\]
Prop 1 (Cancellation 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 cancellation holds in $D$

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

Know $a 0 = 0$

So $a b = a 0$, by cancellation

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

\qed
**Thm:** Every finite integral domain is a field.

**Proof:** Let \( D \) be a finite domain.

\[ D^* = \text{non-zero elements in} \ D \]

Define a map \( \lambda_a : D^* \to D^* \)
\[ d \mapsto da \]
for each \( a \in D^* \)

\[ \lambda_a \text{ is 1-1}: \quad \text{if} \quad \lambda_a(d_1) = \lambda_a(d_2) \]
\[ \Rightarrow \quad ad_1 = ad_2 \Rightarrow \quad d_1 = d_2 \]
by cancellation

\[ \therefore \quad \lambda_a \text{ is onto since } D^* \text{ is a finite set and } \lambda_a \text{ is 1-1} \]

\[ \therefore \exists ! d \in D^* \text{ such that } \lambda_a(d) = ad = 1 \]

\[ \therefore \quad d \text{ is a left inverse of } a, \text{ but } D \text{ is commutative} \]
\[ \therefore \quad ad = da = 1 \quad \therefore \quad a^{-1} = d \]

**Def.** Let \( n \geq 0 \) \( n \in \mathbb{Z} \), \( r \in R \) a ring

write \( \underbrace{n \cdot r}_\text{Just a notation \( \times \) \( n \) times} = \underbrace{r + \cdots + r} \)

The characteristic of \( R \) is
\[ \text{Char} (R) = \text{least positive } n \in \mathbb{Z} \text{ such that } nr = 0 \text{ for all} \]

\[ r + \cdots + r = 0 \quad \text{for } r \in R \]

If no such \( n \) exists, \( = 0 \).

**Example:** \( \text{Char} (\mathbb{Z}_p) = p \) for \( p \) prime.

Since for \( a \in \mathbb{Z}_p \):

\[ a + \cdots + a = p \cdot a = 0 \quad \text{p times} \]

\( \text{Char} (\mathbb{Z}) = \text{Char} (\mathbb{Q}) = \text{Char} (\mathbb{R}) = 0 \)

**Lemma:** Let \( R \) be a ring, \( 1 \in R \). If \( 111 = n \)

then \( \text{Char}(R) = n \).

If \( n \mid 0 \) \( \forall n \to 0 \) \( \text{Char}(R) = 0 \)

**Proof:** \( \text{Set } n < \infty \), \( n \cdot 1 = 1 + \cdots + 1 = 0 \).

Fix \( r \in R \):

\[ nr = n(1r) = n(11) = (1 + \cdots + 1)r = 0 \]

If \( n = \infty \) \( \Rightarrow \) \( 1 + \cdots + 1 \neq 0 \) \( \forall 1 \) \( n \) times

\[ \text{Char}(R) = 0 \]
Theorem: The characteristic of an integral domain is either zero or prime.

Proof:
Let \( D \) be an integral domain, \( \text{Char}(D) = n \neq 0 \).

If \( n \) is not prime \( \Rightarrow n = a \cdot b \), \( 1 \leq a \leq n \), \( 1 \leq b \leq n \).

Since \( \text{Char}(D) = n \), then \( n \cdot 1 = 0 \).

\[ (a \cdot b) \cdot 1 = 0 \]

Up check:
\[ = (a \cdot 1)(b \cdot 1) = 0 \]

\[ \Rightarrow \text{either } a \cdot 1 = 0 \text{ or } b \cdot 1 = 0 \]

\[ \Rightarrow \text{either } \text{Char}(D) = a \text{ or } \text{Char}(D) = b \]

This is a contradiction of \( \text{Char}(D) = n \neq a, b \).

\[ \Rightarrow \text{either } n \text{ is prime or } D \]