Last time:

- Defined and gave examples of subrings.
- Subring test: A subset S of a ring R is a subring if and only if
  (S0) $S \neq \emptyset$.
  (S1) If $a, b \in S$ then $a - b \in S$.
  (S2) If $a, b \in S$ then $a \cdot b \in S$.

Subrings of $R = \mathbb{Z}$.

Question: What are the subrings of $\mathbb{Z}$?

We know that $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \dots, m\mathbb{Z}$.

Are there more than these?

Ex: S = odd numbers. not a subring because it is not closed under addition.

How about $S = \{0, 3, 8, 11, 6, 2, 1, 4, 5, -3, -8, -11, \dots\}$

$= \mathbb{Z}$.

Theorem: The subrings of the ring $\mathbb{Z}$ are exactly

$0\mathbb{Z}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \dots, m\mathbb{Z}, \dots$

$0\mathbb{Z} = \{0\}$

Proof. Let's first prove that all these are indeed subrings of $\mathbb{Z}$.

Consider $S = m\mathbb{Z}$. Let's use the subring test to show that S is a subring of $\mathbb{Z}$.

(S0) $S \neq \emptyset$ because for instance $0 \in S$. $(0 = 0 \cdot m)$

(S1) Suppose $a, b \in S$. This means that we can write $a = m \cdot x$ and $b = m \cdot y$ with $x, y \in \mathbb{Z}$.

(S1) Suppose ...

write $a = m \cdot x$ and $b = m \cdot y$ with $x, y \in \mathbb{Z}$.

Then $a - b = mx - my = m(x-y) \in m\mathbb{Z} = S$

(S2) Suppose $a, b \in S$. This means that we can write $a = mx$ $b = my$ for $x, y \in \mathbb{Z}$.

Then $a \cdot b = mx \cdot my = m(\underbrace{x \cdot m \cdot y}_{\in \mathbb{Z}}) \in m\mathbb{Z} = S$.

We now show that any subring of $\mathbb{Z}$ has to be of the form $m \cdot \mathbb{Z}$ for some m.

Suppose S is a subring of $\mathbb{Z}$.

If $S = \{0\}$ then $S = 0 \cdot \mathbb{Z}$.

If S contains more than just the zero element, as S is closed under negatives, S needs to contain a positive integer.

Let m be the smallest positive integer in S.

We want to show that $S = m \cdot \mathbb{Z}$.

The inclusion $S \supseteq m\mathbb{Z}$ follows because:

since $m \in S$ then $m+m$, $m+m+m$, $m+m+m+m$, ... are elements of S, (as S is closed under addition), and thus $-m$, $-(m+m)$, $-(m+m+m)$, ... are also in S.

- To show that $S \subseteq m\mathbb{Z}$ take any $a \in S$.

Using the division algorithm, we can write

$$a = m \cdot q + r \quad \text{with} \quad 0 \leq \underline{r < m}$$

This means that

$$r = \underbrace{a}_{\in S} - \underbrace{m \cdot q}_{\in S}$$

← must be in S as it is a difference of two elements of S.

Since m was the smallest positive integer in S

Since m was ...

and $r < m$, we must have $r = 0$,

So $a = mq \in m\mathbb{Z}$. $\blacksquare$

- <u>Matrix rings:</u>

If R is any ring, you can construct the ring $M_{n\times n}(R)$ = $n \times n$ matrices with entries in R.

with addition and multiplication of matrices as usual.

<u>Ex</u>: $R = \{T, F\}$. addition : XOR $+$
$\{1, 0\}$ multiplication : AND $\cdot$

$\underbrace{T \overset{+}{\text{XOR}}\, T = F}_{T \text{ is the negative of } T.}$.

$F \overset{+}{\text{XOR}}\, F = F$
$F \overset{+}{\text{XOR}}\, T = T$ $\Big\}$ F is the zero.

We can construct $M_{3\times 3}(\{T, F\})$:

$$\begin{pmatrix} T & F & F \\ F & F & T \\ T & F & T \end{pmatrix} \underset{+}{\text{XOR}} \begin{pmatrix} F & T & T \\ F & F & T \\ F & T & T \end{pmatrix} = \begin{pmatrix} T & T & T \\ F & F & F \\ T & T & F \end{pmatrix}$$

$$\begin{pmatrix} T & F & F \\ F & F & T \\ T & F & T \end{pmatrix} \underset{\cdot}{\text{AND}} \begin{pmatrix} F & T & T \\ F & F & T \\ F & T & T \end{pmatrix} = \begin{pmatrix} F & T & T \\ F & T & T \\ F & F & F \end{pmatrix}$$

This satisfies all the axioms of a ring.

- <u>Exercises</u>:

(1). Given the following ring R and subset S, determine whether S is a subring of R.

(a) $R = \mathbb{C}$ $S = \{ a+bi \mid a,b \in \mathbb{Z} \}$.

(b) $R = M_{n\times n}(\mathbb{R})$ $S = \{$ invertible matrices $\}$.

(c) $R = \mathbb{R}[x]$ $S = \{ f \in \mathbb{R}[x] \mid f'(0) = 0 \}$

what about $f'(1) = 0$?

what about $f'(0) = 1$?

(2) Prove that in any ring,

$(-1)\cdot a = -a$. for any $a \in R$.

(1b) No. Using the subring test, we see that S fails (S1):

For instance $I \in S$, $I \in S$ but $I - I = 0 \notin S$

I: $n\times n$ identity matrix

0: zero matrix.

(1c) Yes. Let's use the subring test.

(S0) S is not empty because $S = \{0,$ constants, x^2+1, x^3+x^2, $\}$

(S1) Suppose $f, g \in S$. This means that $f'(0) = 0$ and $g'(0) = 0$. Then $(f-g)'(0) = f'(0) - g'(0)$

$= 0 - 0 = 0$.

so $f - g \in S$.

(S2) Suppose $f, g \in S$. This means that $f'(0) = 0$

(S2) Suppose $f, g \in S$. This means that $f'(0) = 0$

$g'(0) = 0$. Then $(f \cdot g)'(0) = f(0) \cdot \cancel{g'(0)}^{\,0} + \cancel{f'(0)}^{\,0} \cdot g(0)$

$= 0 + 0 = 0$

So $f \cdot g \in S$.