Lecture 3

29 January 2024 14:00

Last time: Basic properties of rings

- The zero element is unique
- Additive inverses are unique (notation $-a$)
- Cancellative law for addition

Proposition: For any $a \in R$

$$-(-a) = a$$

Proof: We need to show that a is the additive inverse to $-a$, meaning

$$(-a) + a = 0$$

But this is true by the definition of $-a$.

Proposition: For any $a \in R$ we have

$$a \cdot 0 = 0$$

$$0 \cdot a = 0$$

Proof:

$$a \cdot 0 \overset{\text{zero axiom (A2)}}{=} a \cdot (0+0)$$

$$\overset{(D)}{=} (a \cdot 0) + (a \cdot 0)$$

So $\overset{\text{// zero axiom (A2)}}{0 + a \cdot 0} = a \cdot 0 + a \cdot 0$.

Using the cancellative laws we conclude that

$$0 = a \cdot 0.$$

Exercise: Prove that $0 \cdot a = 0$.

Exercise: Prove that

$$(-a) \cdot b = -(a \cdot b)$$

$$(-a)\cdot b = -(a\cdot b)$$

Subrings:

Definition: Suppose R is a ring. A subset $S \subseteq R$ is called a subring of R if S itself is a ring with the same operations as R.

Examples:

- Take $R = \mathbb{Z}$. A subring of R is $S = 2\mathbb{Z}$.
- Take $R = \mathbb{Q}$.

  $S = \mathbb{Z}$ is a subring.

  not subring $\rightarrow$ $S = \frac{1}{2}\mathbb{Z} = \left\{ \frac{m}{2} : m \in \mathbb{Z} \right\}$ Is this a subring? NO.

  $S = \left\{ \frac{m}{2n} : m, n \in \mathbb{Z} \right\}$. is a subring of $\mathbb{Q}$ (in fact equal to all of $\mathbb{Q}$)

  $S = \left\{ \frac{m}{2^k} : \begin{matrix} m \in \mathbb{Z} \\ k \in \mathbb{Z}_{\geq 0} \end{matrix} \right\}$ is a subring of $\mathbb{Q}$.

- Take $R = \mathbb{Z}$

  $S = \{0, 1, 2, \dots, n-1\}$ with addition and multiplication modulo n.

  S is a subset but is not a subring since the operations in S

subring since the operations in ~ are not the same operations as in R:

If $n=7$, for example,

in S: $3+6=2$

in R: $3+6=9$

different elements of R

- Take $R = M_{n\times n}(\mathbb{Z})$.

  $S =$ upper triangular matrices is a subring.

- Example: Any ring R has at least two subrings:

  $S = R$ and $S = \{0\}$ ↳ zero element.

- What properties does a subset $S \subseteq R$ ring. need to satisfy to be a subring?

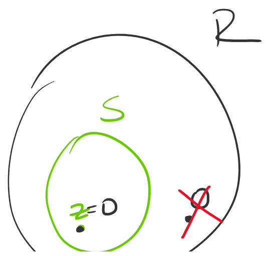
(A0) Closure for addition: $\boxed{\text{If } a,b \in S \text{ then } a+b \in S.}$

(A1) Associativity for addition: If $a, b, c \in S$ then

$$a+(b+c) = (a+b)+c$$

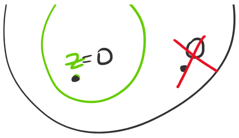
Automatic since R satisfies associativity

(A2) Zero law: There is an element $z \in S$ such that for any $a \in S$ $a+z=a$.



Taking this as an equation about elements in R, using the cancellative

Taking this as an equation
elements in R, using the cancellative
law in R we conclude $z = 0$.



(A2) is saying $0 \in S$.
→ the zero of R

(A3) Negation law: For any $a \in S$ there exists $b \in S$ such that $a + b = 0$
↪ zero of S = zero of R.

Thinking of this as an equation in R, we know that $b = -a$.

(A3) is saying if $a \in S$ then $-a \in S$.

(A4) Commutativity of addition: For any $a, b \in S$ $a + b = b + a$.

Automatic as addition in R is commutative.

(M0) Closure for multiplication: If $a, b \in S$ then $a \cdot b \in S$.

(M1) Associativity for multiplication:

Automatic as R satisfies (M1).

(D) Distributivity:

Automatic as R satisfies (D).

Theorem (the subring test)

Let R be a ring and S a subset of R. Then S is a subring of R if and only if it satisfies the following properties:

(S0) $S \neq \emptyset$.

(S1) If $a, b \in S$ then $\underbrace{a - b}_{a + (-b)} \in S$.

(S2) If $a, b \in S$ then $a \cdot b \in S$.

Proof: ($\Longrightarrow$) Suppose S is a subring of R. S satisfies (S0) because S must contain 0.

Proof: ($\Rightarrow$) Supp

S satisfies (S0) because S must contain 0.

S satisfies (S1) because if $a, b \in S$ then $-b \in S$ (by (A3))

and so $\underset{\text{in } S}{\underset{\downarrow}{a}} + (\underset{\text{in } S}{\underset{\downarrow}{-b}}) = \underbrace{a-b} \in S$ (by (A0)).

$\Rightarrow$ in S.

S satisfies (S2) because it satisfies (M0).

($\Leftarrow$): Suppose S satisfies (S0), (S1), (S2). We want to prove S is a subring.

- S must contain the zero element (of R) because by (S0) there exists some $a \in S$, and by (S1) we have $\underset{0}{\underset{\parallel}{a-a}} \in S$. So S satisfies (A2).
- S is closed under negation because if $a \in S$, since $0 \in S$, then by (S1) we have $\underbrace{0-a}_{-a} \in S$. S satisfies (A3).
- S is closed under addition because if $a, b \in S$ then $-b \in S$ (by (A3)), and by (S1) we get $\underset{\underset{\underset{a+b}{\parallel}}{a+(-(-b))}}{\underset{\parallel}{a-(-b)}} \in S$. So S satisfies (A0).
- S satisfies (M0) because it satisfies (S2). ∎

Subrings of $\mathbb{Z}$:

- Example: $S = \mathbb{Z}$, $S = \{0\}$, $S = 2\mathbb{Z}$, $S = 5 \cdot \mathbb{Z}$.
- Proposition: If $m \in \mathbb{Z}$ then $S = m \cdot \mathbb{Z}$ is a subring

of $R = \mathbb{Z}$.

<u>Proof</u>:

We need to show that S satisfies $(S0), (S1), (S2)$.

- $(S0)$ $S \neq \emptyset$ as S contains, for example, 0.
- $(S1)$ If $a, b \in S$ then $\exists\, k, l \in \mathbb{Z}$ such that $a = k \cdot m$ and $b = l \cdot m$.

  Then $a - b = km - l \cdot m = \underbrace{(k - l)}_{\in \mathbb{Z}} \cdot m$, so $a - b \in \underset{\substack{\shortparallel \\ S}}{m\mathbb{Z}}$.
- $(S2)$ If $a, b \in S$ then $\exists\, k, l \in \mathbb{Z}$ such that

  $a = k \cdot m \quad b = l \cdot m$

  Then $a \cdot b = k \cdot m \cdot l \cdot m = \underbrace{(k\,m\,l)}_{\in \mathbb{Z}} \cdot m$ so $a \cdot b \in \underset{\substack{\shortparallel \\ S}}{m\mathbb{Z}}$. ■

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

  If $m = 1$ then $S = \mathbb{Z} = 1 \cdot \mathbb{Z}$.
- Are these subrings commutative? Yes.
- Do these subrings have an identity? No, unless $m = \pm 1$ (so $S = \mathbb{Z}$).
- Are these division rings? No.