Lecture 2

26 January 2024 16:10

Last time:

- Formal definition of a ring satisfying axioms (A0) - (A4), (M0) - (M1), (D).

  Optional axioms (M2) - (M4).

---

## Basic properties of rings

Proposition: In any ring $R$, the following identity holds:

$$(a+b)^2 = a^2 + a\cdot b + b\cdot a + b^2$$

Proof: Let's start from the left hand side:

$$(a+b)^2 \overset{\text{definition of square}}{=} (a+b)\cdot(a+b)$$

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

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

$$= a^2 + b\cdot a + a\cdot b + b^2$$

no need for parentheses as + is associative

$$\overset{(A4)}{=} a^2 + a\cdot b + b\cdot a + b^2$$

∎

---

Proposition: In any ring $R$, the zero element is unique (this is why it is called the zero element).

Proof: Suppose $z_1, z_2$ are two elements of $R$

such ... $a + z_1 = a \quad \forall a \in R$

Proof: Suppose $z_1, z_2$

satisfying

$$a + z_1 = a \quad \forall a \in R$$
$$z_1 + a = a \quad \forall a \in R \quad (*)$$

$$a + z_2 = a \quad \forall a \in R \quad (**)$$
$$z_2 + a = a \quad \forall a \in R.$$

Consider the sum $z_1 + z_2$.

Because of $(*)$, $z_1 + z_2 = z_2$

Because of $(**)$, $z_1 + z_2 = z_1$

So $z_1 = z_1 + z_2 = z_2$ and $z_1 = z_2$ ∎

---

Proposition: If $a$ is an element of a ring $R$, then the additive inverse of $a$ is unique. We denote this element by $-a$.

Proof: Suppose $b$ and $c$ are both additive inverses to $a$. This means

$$\left.\begin{aligned} a+b &= 0 \\ (*) \quad b+a &= 0 \end{aligned}\right\} \text{ b is an additive inverse of a}$$

$$\left.\begin{aligned} (**) \quad a+c &= 0 \\ c+a &= 0 \end{aligned}\right\} \text{ c is an additive inverse of a.}$$

Take $(*)$ and add $c$ on the right:

$$
\begin{aligned}
(b+a)+c &= 0+c \\
&\downarrow (A1) \qquad \downarrow (A2) \\
b+(a+c) &= c \\
&\downarrow (**) \\
b+0 &= c \\
&\downarrow (A2) \\
b &= c
\end{aligned}
$$

$\blacksquare$

---

<u>Definition</u>. In any ring, we denote

$$a - b := a + \underbrace{(-b)}_{\text{additive inverse of } b.} .$$

---

<u>Proposition</u>: In any ring $R$, there is cancellation for addition: (called cancellation law for addition).

If $\cancel{a} + b = \cancel{a} + c$

then $b = c$.

<u>Proof</u>: Suppose $a + b = a + c$

Adding $-a$ on both sides we get

$$
\begin{aligned}
-a + (a+b) &= -a + (a+c) \\
&\downarrow (A1) \\
(-a+a)+b &= (-a+a)+c \\
&\downarrow \text{def of } -a \\
0 + b &= 0 + c \\
&\downarrow (A2) \\
b &= c.
\end{aligned}
$$

$\blacksquare$

---

**Question:** Is the cancellative law for multiplication true in general?

$$a \cdot b = a \cdot c \overset{?}{\Longrightarrow} b = c$$

Definitely not if $a = 0$.

⚠ Not true in general!!

$$\underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{a} \cdot \underbrace{\begin{pmatrix} 3 & 7 \\ 0 & 0 \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{a} \cdot \underbrace{\begin{pmatrix} -2 & 1 \\ 0 & 0 \end{pmatrix}}_{c}$$

We cannot conclude that $b = c$.

---

**Exercise:**

| | (A0) | A1 | A2 | A3 | A4 | (M0) | M1 | D | M2 | M3 | M4 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbb{N} = \{0, 1, 2, \dots\}$ | | | | | | | | | | | | 2 F |
| Polynomials with coefficients in $\mathbb{Z}$ $\mathbb{Z}[x]$ | | | | | | | | | | | | 1 F |
| Polynomials $\mathbb{R}[x]$ of degree $\leq 4$ | T | T | T | T | T | F | T | T | T | F | T | 2 F * |
| Polynomials $\mathbb{Z}[x]$ with constant term $= 0$ | | | | | | | | | | | | 2 F |
| Integers $\mathbb{Z}$ divisible by 3 | | | | | | | | | | | | 2 F |
| Invertible 2x2 matrices with real entries | F | T | F | • | T | T | T | T | T | T | F | 3 F * |
| Upper triangular 2x2 matrices entries in $\mathbb{R}$ | T | T | T | T | T | T | T | T | T | F | F | 2 F |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Upper triangular 2x2 matrices entries in $\mathbb{R}$ | T | T | T | T | T | T | T | T | T | F | F |

2F