前提知識

集合とは, いくつかのものをひとまとめにして考えた“ものの集まり”のことである. 例えば「自然数全ての集まり」や「0 以上 1 以下の実数全体の集まり」などは, いずれも集合である.

A が 1 つの集合であるとき, A の中に入っている個々の“もの”を A の**元**または**要素**という. 「もの」a が集合 A の元であることを, 記号で

$$a \in A \text{ または } A \ni a$$

で表す.

群

定義 0.0.1 | 〈 群 〉

集合 G が演算「$\cdot$」において**群**であるとは, G の任意の 2 元 a, b において $a \cdot b \in G$ であり, 以下の性質を満たすことをいう.
(G1) G の任意の元 a, b, c において, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ.
(G2) G の任意の元 a に対して, $a \cdot e = e \cdot a = a$ となる元 $e \in G$ が存在する.
(G3) G の任意の元 a に対して, $a \cdot a^{-1} = a^{-1} \cdot a = e$ となる元 $a^{-1} \in G$ が存在する.

例えば, 整数全体の集合 $\mathbb{Z}$ は演算「+」において群である. 実際, 上の定義の G を $\mathbb{Z}$, e を 0, a^{-1} を $-a$ とすると, 整数全体では (G1)-(G3) が成り立つ. 具体的には以下の通りである.
(G1) 任意の整数 a, b, c において, $(a + b) + c = a + (b + c)$ が成り立つ.
(G2) 任意の整数 a に対して, $a + 0 = 0 + a = a$ となる整数 0 が存在する.
(G3) 任意の整数 a に対して, $a + (-a) = (-a) + a = 0$ となる元 $-a$ が存在する.

....

余裕がある人は以下の問いを考えてみてほしい.

- 自然数全体の集合 $\mathbb{N}$ は群であるか?
- 有理数 (分数) 全体の集合 $\mathbb{Q}$ は群であるか?
- 実数全体の集合 $\mathbb{R}$ は群であるか?

前提知識

集合とは, いくつかのものをひとまとめにして考えた "ものの集まり" のことである. 例えば「自然数全ての集まり」や「0 以上 1 以下の実数全体の集まり」などは, いずれも集合である.

A が 1 つの集合であるとき, A の中に入っている個々の "もの" を A の**元**または**要素**という. 「もの」a が集合 A の元であることを, 記号で

$$a \in A \text{ または } A \ni a$$

で表す.

環

定義 0.0.2 | 〈 環 〉

集合 R が演算「$+, \cdot$」において**環**であるとは, R の任意の 2 元 a, b において $a \cdot b \in R$ であり, 以下の性質を満たすことをいう.

(R0) R は演算 $+$ において可換群である. (ここは他の人の担当であるため, 一旦認めて良い)

(R1) R の任意の元 a, b, c において, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ.

(R2) R の任意の元 a に対して, $a \cdot e = e \cdot a = a$ となる元 $e \in G$ が存在する.

(R3) R の任意の元 a, b, c に対して, $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ が成り立つ.

例えば, 整数全体の集合 $\mathbb{Z}$ は演算「$+, \times$」において環である. 実際, $\mathbb{Z}$ は可換群であり, 上の定義の R を $\mathbb{Z}$, e を 1 とすると, 整数全体では (R1)-(R3) が成り立つ. 具体的には以下の通りである.

(R1) 任意の整数 a, b, c において, $(a \times b) \times c = a \times (b \times c)$ が成り立つ.

(R2) 任意の整数 a に対して, $a \times e = e \times a = a$ となる整数 1 が存在する.

(R3) 任意の整数 a, b, c に対して, $a \times (b + c) = a \times b + a \times c$, $(a + b) \times c = a \times c + b \times c$ が成り立つ.

………………………………………………………………………………………

余裕がある人は以下の問いを考えてみてほしい. なお, 可換群であることは認めてよい.

- 有理数 (分数) 全体の集合 $\mathbb{Q}$ は環であるか?
- 実数全体の集合 $\mathbb{R}$ は環であるか?

前提知識

集合とは, いくつかのものをひとまとめにして考えた "ものの集まり" のことである. 例えば「自然数全ての集まり」や「0 以上 1 以下の実数全体の集まり」などは, いずれも集合である.

A が 1 つの集合であるとき, A の中に入っている個々の "もの" を A の**元**または**要素**という. 「もの」a が集合 A の元であることを, 記号で

$$a \in A \text{ または } A \ni a$$

で表す.

可換及び 0 をかけると 0 になる証明

可換

定義 0.0.3 | 〈 可換 〉

集合 X が演算「$\cdot$」において**可換**であるとは, X の任意の 2 元 a, b において $a \cdot b = b \cdot a$ を満たすことをいう. 可換な群を**可換群**という.

例えば, 整数全体の集合 $\mathbb{Z}$ は演算「$+$」において可換である. 実際, 任意の整数 a, b は $a + b = b + a$ を満たす.

0 をかけると 0 になる証明

整数全体の集合 $\mathbb{Z}$ は演算「$+, \times$」において環であり, 以下の性質を満たす. (ここは他の人の担当であるため, そういうものであると認めて良い)
(G2) 任意の整数 a に対して, $a + 0 = 0 + a = a$ となる整数 0 が存在する.
(G3) 任意の整数 a に対して, $a + (-a) = (-a) + a = 0$ となる元 $-a$ が存在する.
(R3) 任意の整数 a, b, c に対して, $a \times (b + c) = a \times b + a \times c$, $(a + b) \times c = a \times c + b \times c$ が成り立つ.
このとき以下の事実が証明できる.

定理 0.0.4

任意の整数 $a \in \mathbb{Z}$ に対して, $a \times 0 = 0$

Proof.

$$\begin{aligned}
& & a \times 0 &= a \times (0 + 0) && \text{(G2) を左辺の 0 に適用} \\
& & &= a \times 0 + a \times 0 && \text{(R3) を適用} \\
&\Rightarrow & a \times 0 + (-(a \times 0)) &= a \times 0 + a \times 0 + (-(a \times 0)) && \text{(G3) に } (a \times 0) \text{ を適用し, 両辺に加える} \\
&\Rightarrow & 0 &= a \times 0 && \text{(G3) を適用} \\
&\Rightarrow & a \times 0 &= 0 && \text{右辺と左辺を入れ替え}
\end{aligned}$$

□