

群論

Anko

2023 年 11 月 22 日

目次

1	群に触れる	2
1.1	群ってなんだろう？	2
1.2	部分群と生成元	3
1.3	位数	4
1.4	剰余群	4

1 群に触れる

1.1 群ってなんだろう？

定義 (群).

空集合でない集合 G 上で単位元と逆元を持つ結合的な演算が定義されているとき G を群という。演算 \cdot

$$ae = ea = a \quad (1)$$

$$aa^{-1} = a^{-1}a = e \quad (2)$$

$$(a + b) + c = a + (b + c) \quad (3)$$

これはもう覚えるしかないです。

「単位元と逆元を持つ結合的な演算」

と覚えてください。

まずは足し算 $+$ の群を探しに行きます。

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z} \supset 2\mathbb{Z} \supset \{0\}$$

これらが群となっているのは単位元と逆元を持つ結合的な演算であることを調べればいいです。

1. $(a + b) + c = a + (b + c)$
2. $e := 0, a^{-1} := -a$

次に掛け算 \times の群はどうでしょう。

$$\mathbb{C}^\times \supset \mathbb{R}^\times \supset \mathbb{Q}^\times \supset \mathbb{Z}^\times \supset \{1\}$$

右肩に \times があるのは掛け算に使えない元を取り除いたものと考えればいいです。(環の乗法群) 例えば実数 \mathbb{R} は 0 の逆元はないのでそれを取り除いたものです。以下のように大体の代数では 0 だけを除いたものと思えばいいですが、整数 \mathbb{Z} は例外でほとんどの整数の逆元は分数となってしまって整数に戻ってきません。辛うじて ± 1 の逆元は $\pm 1 \in \mathbb{Z}$ なので整数に入って

$$\mathbb{C}^\times = \mathbb{C} \setminus \{0\} \quad (4)$$

$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\} \quad (5)$$

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\} \quad (6)$$

$$\mathbb{Z}^\times = \{\pm 1\} \quad (7)$$

これらが群となっているのは単位元と逆元を持つ結合的な演算であることを調べればいいです。

$$1. (a \times b) \times c = a \times (b \times c)$$

$$2. e := 1, a^{-1} := \frac{1}{a}$$

群というのはこのようなものです。

準同型定理、表現論などとても豊富な性質があります。一つでも条件を外すと (それらの研究をしている人には申し訳ないが) 殺風景となってしまいます。最小の条件でもっとも幅広い分野に適用できる代数構造というのが群なのです。

可換法則 $ab = ba$ が成り立つとき可換群という。

環や体は和と積

1.2 部分群と生成元

定義 (部分群).

群 G の部分集合 H が群となると H は G の部分群であるという。

定義.

G を群として $g \in G$

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\} \quad (8)$$

一般的な代数を扱っているのに整数が入っているのか！？ ってのを気づいて欲しい。

例えば加法群 \mathbb{Z} において $2 \in \mathbb{Z}$ の巡回部分群は

$$\langle 2 \rangle = \{2n \mid n \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} = 2\mathbb{Z} \subset \mathbb{Z} \quad (9)$$

これが群となっていることがわかるでしょう。

乗法群 \mathbb{Q}^\times において $2 \in \mathbb{Q}^\times$ の巡回部分群は

$$\langle 2 \rangle = \{2^n \mid n \in \mathbb{Z}\} = \left\{ \dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8 \dots \right\} \subset \mathbb{Q} \quad (10)$$

1.3 位数

定義 (群の位数).

群 G の濃度 $|G|$ を群 G の位数という。

また G について $|G| < \infty$ のとき有限群, $|G| \geq \infty$ のとき無限群という。

1.4 剰余群