

今日のテーマ 部分群

群の部分群とは、部分集合であって群になっているもののことである。
ただし、部分群の掛け算はもとの群の掛け算と一致しなければならない。

部分群の定義に入る前に、群の定義から直ちに導かれる性質についていくつか述べてみよう。以下では G の演算 $m(x, y)$ を単に xy と書くことにする。

定理 2.1. G は群であるとする。このとき、

- (1) G の単位元はただ一つである。
- (2) G の元 x を一つとってくると、その逆元はただ一つである。(これを普通 x^{-1} と書く。)
- (3) $x \in G$ に対して、 $(x^{-1})^{-1} = x$ が成り立つ。
- (4) $a, b, c \in G$ が $ab = cb$ を満たすなら、必ず $a = c$ が成り立つ。
- (5) 任意の $a, b \in G$ に対して、 $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。
- (6) 任意の $a, b, c, d \in G$ に対して、

$$((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d) = (a(bc))d$$

が成り立つ。すなわち 4 つの元のかげ算は a, b, c, d の順番のみに依り、かけ算の順番には依らない。(この積のことを普通単に $abcd$ と書く) (もっとたくさんの元の積についても同様のことが成り立つ。)

定義 2.1 (群の元のべき乗). G を群、 x をその一つの元とする。

- (1) 自然数 n に対して、 x^n (《 x の n -乗》) は帰納的に次のように定義される。

$$\begin{aligned} x^0 &= e \text{ (単位元)}, \\ x^{n+1} &= x^n x \end{aligned}$$

- (2) n が負の整数のときには、 x^n は x^{-n} の逆元として定義する。

定理 2.2. $x^m x^n = x^{m+n}$

さて、本題に入る。部分群の正確な定義は次のようになる。

定義 2.2 (部分群の定義). 群 (G, m) が与えられているとする。 G の部分集合 H が G の部分群であるとは、次の条件を満たすときに言う。

(0) 掛け算 $m: G \times G \rightarrow G$ を $H \times H$ に制限すると、これは H に値を持つ。すなわち、次のような写像が誘導される。

$$m: H \times H \rightarrow H$$

- (1) (H, m) は群である。

条件 (0) は次のように言い換えても良い。

(0') h, k を H から任意に取ってくると、いつでも $m(h, k)$ は H の元である。

例 2.1. 次の集合はそれぞれ $(\mathbb{Z}, +)$ の部分群である。

- (1) \mathbb{Z} 自身。
- (2) $\{0\}$.
- (3) 偶数全体の集合 $2\mathbb{Z}$.
- (4) 3 の倍数全体の集合 $3\mathbb{Z}$.

次の集合はそれぞれ $(\mathbb{Q}^\times, \times)$ の部分群である。

- (1) \mathbb{Q}^\times 自身。
- (2) $\{1\}$.
- (3) $\{\pm 1\}$.
- (4) $\{2^n; n \in \mathbb{Z}\} (= \{1, 2, 4, 8, 16, 32, \dots\} \cup \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \dots\})$
- (5) $\{2^m 3^n; m, n \in \mathbb{Z}\}$

例 2.2. 次の集合はどれも群 $(\mathbb{Z}, +)$ の部分群 でない。

- (1) 奇数全体の集合 $2\mathbb{Z} + 1$.
- (2) $\{\pm 1\}$.

定理 2.3. G の部分群 H が与えられたとする。このとき H の単位元は G の単位元と一致し、 H の元 h の H での逆元は G での逆元と一致する。

定理 2.4. 群 G の部分集合 H が G の部分群であるためには、次の三条件が満足されることが必要十分である。

- (1) $a, b \in H \implies ab \in H$
- (2) $e \in H$
- (3) $a \in H \implies a^{-1} \in H$

定理 2.5. (今回は証明の一部分だけをやる。) \mathbb{Z} の部分群は必ず

$$n\mathbb{Z} \quad (= n \text{ の倍数の集合}) \quad (n = 0, 1, 2, 3, \dots)$$

のどれかである。(もちろん、 $n\mathbb{Z}$ は \mathbb{Z} の部分群になっている。)

レポート問題

次の中から一問を選んで、レポートとして提出しなさい。

(期限：次の講義の終了時まで。)

- (I) 実数の乗法群 $(\mathbb{R}^\times, \times)$ の部分集合だが部分群にはならない例を一つ挙げなさい。(オリジナルであること)