

### 3 有限アーベル群の指標

ここでは有限アーベル群の指標理論について解説する。調べたい対象があまりにも抽象的な場合、それを直接調べるのではなく、別の対象を経由したり、その上に定義された関数などを調べることでもとの情報を復元しようとする手法をとることがよくある。

#### ● 3-1 : アーベル群の指標群

**定義 3.1.** アーベル群  $G$  の **指標** とは、以下の条件を満たす関数  $\chi : G \rightarrow \mathbb{C}$  である。

(CA1) 任意の  $x, y \in G$  に対して,  $\chi(xy) = \chi(x)\chi(y)$ .

(CA2) 任意の  $x \in G$  に対して,  $\chi(x) \neq 0$ .

還元すれば,  $\chi$  は  $G$  からトーラス  $\mathbb{C}^\times$  への群準同型写像である.  $G$  の指標全体を  $\widehat{G}$  とおく.

アーベル群  $G$  に対して,  $\chi, \chi' \in \widehat{G}$  に対して, 関数としての積  $\chi\chi'$  は再び  $G$  の指標である. 実際, 任意の  $x, y \in G$  に対して

$$\chi\chi'(xy) = \chi(xy)\chi'(xy) = \chi(x)\chi(y)\chi'(x)\chi'(y) = \chi(x)\chi'(x)\chi(y)\chi'(y) = \chi\chi'(x)\chi\chi'(y)$$

だから (CA1) を満たす. また, 任意の  $x \in G$  に対して,  $\chi(x) \neq 0, \chi'(x) \neq 0$  だから  $\chi\chi'(x) \neq 0$  となるので (CA2) が成り立つ. 以上で  $\chi\chi' \in \widehat{G}$  である. この積について  $\widehat{G}$  はアーベル群であり,  $G$  の **指標群** という.

**補題 3.2.**  $G$  が位数  $n$  の巡回群であるとき,  $\widehat{G}$  も位数  $n$  の巡回群である. 特に,  $G \simeq \widehat{G}$  が成り立つ.

**証明.**  $G$  の生成元を  $a \in G$  とする.  $\chi \in \widehat{G}$  を任意にとる. このとき,  $G$  が位数  $n$  の巡回群なので,  $a^n = 1$  である. このとき, (CA1) より

$$\chi(1) = \chi(a^n) = \chi(a)^n$$

である. ところで,  $\chi(1) = \chi(1^2) = \chi(1)^2$  であって, (CA2) から  $\chi(1) \neq 0$  だから  $\chi(1) = 1$  を得る. よって,  $\chi(a)^n = 1$  だから  $\chi(a)$  は 1 の  $n$  乗根である. そこで, 写像  $\phi : \widehat{G} \rightarrow U_n$  を

$$\phi : \widehat{G} \ni \chi \mapsto \chi(a) \in U_n$$

考えれば, これは全単射な群準同型写像である. 実際, 群準同型写像であることは,  $\chi, \chi' \in \widehat{G}$  を任意にとれば

$$\phi(\chi\chi') = \chi\chi'(a) = \chi(a)\chi'(a) = \phi(\chi)\phi(\chi')$$

から従う. 単射であることを確認しよう.  $\chi, \chi' \in \widehat{G}$  が  $\phi(\chi) = \phi(\chi')$  であるとする. つまり,  $\chi(a) = \chi'(a)$  とする. このとき,  $a \in G$  は生成元なので, 任意の  $x \in G$  は  $x = a^k$  となるような  $k \in \mathbb{Z}$  がとれるが, (CA1) より

$$\chi(x) = \chi(a^k) = \chi(a)^k = \chi'(a)^k = \chi'(a^k) = \chi'(x)$$

がわかるので,  $\chi = \chi'$  である. よって,  $\phi$  は単射である. 次に,  $\phi$  が全射であることを示そう. 任意に  $\xi \in U_n$  をとる. このとき,  $\chi : G \rightarrow \mathbb{C}$  を,  $x = a^k \in G$  に対して

$$\chi(a^k) = \xi^k$$

と定義すれば,  $\chi \in \widehat{G}$  である. この  $\chi$  について  $\phi(\chi) = \chi(a) = \xi$  なので  $\phi$  は全射であることがわかった. 以上で,  $\phi$  は群同型写像となる. 従って,  $\widehat{G}$  は位数  $n$  の巡回群であり,  $G \simeq \widehat{G}$  がわかった.  $\square$

**補題 3.3.**  $G_1, G_2$  をアーベル群とする.  $G = G_1 \times G_2$  とおく. このとき, 群の同型  $\widehat{G} \simeq \widehat{G}_1 \times \widehat{G}_2$  が成り立つ.

**証明.** 任意に  $\chi \in \widehat{G}$  に対して,  $\chi_1 : G_1 \rightarrow \mathbb{C}$  と  $\chi_2 : G_2 \rightarrow \mathbb{C}$  を,  $g \in G_1, h \in G_2$  に対して,

$$\chi_1(g) = \chi(g, 1), \quad \chi_2(h) = \chi(1, h)$$

で定義する. このとき, 各  $i = 1, 2$  に対して,  $\chi_i \in \widehat{G}_i$  がわかる. 写像  $\phi : \widehat{G} \rightarrow \widehat{G}_1 \times \widehat{G}_2$  を

$$\phi(\chi) = (\chi_1, \chi_2)$$

と定義すればこれは群同型写像を定める. (定義に従って, 各自で確かめよ.) よって, 群の同型  $\widehat{G} \simeq \widehat{G}_1 \times \widehat{G}_2$  が成り立つ.  $\square$

任意の有限アーベル群は, 有限個の巡回群の直積に同型であることが知られている (有限アーベル群の構造定理) ので, 次の主張がわかった.

**定理 3.4.**  $G$  が有限アーベル群であるとき, 群の同型  $G \simeq \widehat{\widehat{G}}$  が成り立つ.

これにより, アーベル群  $G$  というのはその指標群  $\widehat{G}$  がわかれば完全にわかる, ということを述べている. 還元すれば, 指標群をみればもとの群がわかる, ということである.

### ● 3-2 : アーベル群の指標の直交関係

有限アーベル群  $G$  上の指標群  $\widehat{G}$  は再びアーベル群であったが, この単位元を  $\varepsilon$  で表し, **単位指標** と呼ぶ. 単位指標  $\varepsilon$  は, 任意の  $g \in G$  に対して  $\varepsilon(g) = 1$  となるような  $G$  の指標である.

**補題 3.5.**  $G$  を有限アーベル群とする. このとき,  $\chi \in \widehat{G}$  に対して

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & (\chi = \varepsilon) \\ 0 & (\chi \neq \varepsilon) \end{cases}$$

ここで, 和は  $G$  の各元  $g$  を全てわたる.

**証明.**  $\chi = \varepsilon$  のときは,

$$\sum_{g \in G} \varepsilon(g) = \sum_{g \in G} 1 = |G|$$

なので, 両辺を  $|G|$  で割れば

$$\frac{1}{|G|} \sum_{g \in G} \varepsilon(g) = 1$$

である.

次に,  $h \in G$  をひとつ固定しておく.  $\chi \in \widehat{G}$  をとろう.  $g$  が  $G$  の元すべてをはしるとき,  $gh$  は  $G$  の元すべてをはしるので

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(gh) = \left( \sum_{g \in G} \chi(g) \right) \chi(h)$$

この式より,  $\chi(h) \neq 1$  であるような  $h \in G$  が存在しないときには

$$\sum_{g \in G} \chi(g) = 0$$

である.  $\square$

ふたつの指標が同じか異なるかを与えるものが, 次の直交関係である.

**定理 3.6.**  $G$  を有限アーベル群として,  $\chi, \chi' \in \widehat{G}$  とする. このとき,

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)} = \begin{cases} 1 & (\chi = \chi') \\ 0 & (\chi \neq \chi') \end{cases}$$

が成り立つ.

**証明. 補題 3.5** を  $\chi$  として  $\chi\chi'^{-1}$  に対して適用すると

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'^{-1}(g) = \begin{cases} 1 & (\chi\chi'^{-1} = \varepsilon) \\ 0 & (\chi\chi'^{-1} \neq \varepsilon) \end{cases}$$

が成り立つ. さて, 任意の  $g \in G$  に対して  $\chi'^{-1}(g) = \chi'(g)^{-1}$  である. また,  $G$  は有限群であるから  $g^n = 1$  となるような  $n$  が存在するから,  $\chi'(g)^n = 1$  が成り立つ. 従って,  $|\chi'(g)| = 1$  である. 従って,  $\chi'(g) \overline{\chi'(g)} = 1$  だから

$$\chi'^{-1}(g) = \overline{\chi'(g)}$$

が成り立つ. よって,

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)} = \begin{cases} 1 & (\chi\chi'^{-1} = \varepsilon, \text{すなわち}, \chi = \chi') \\ 0 & (\chi\chi'^{-1} \neq \varepsilon, \text{すなわち}, \chi \neq \chi') \end{cases}$$

が成り立つ. □

### ● 3-3 : ベクトル空間とエルミート内積

集合  $V$  上に「和」と呼ばれる二項演算

$$+ : V \times V \ni (u, v) \mapsto u + v \in V$$

が定義されており,  $V$  は和  $+$  によってアーベル群であるとする. また,  $c \in \mathbb{C}$  と  $v \in V$  に対して,  $v$  の  $c$  によるスカラー倍  $cv \in V$  が定められているとする.  $V$  が, 次の条件を満たすとき,  $V$  を  $\mathbb{C}$  上の **ベクトル空間** と呼ぶ.

- (V1) 任意の  $c \in \mathbb{C}$  と任意の  $u, v \in V$  に対して,  $c(u + v) = cu + cv$  が成り立つ.
- (V2) 任意の  $c, c' \in \mathbb{C}$  と任意の  $u \in V$  に対して,  $(c + c')u = cu + c'u$  が成り立つ.
- (V3) 任意の  $u \in V$  に対して,  $1u = u$  が成り立つ.
- (V4) 任意の  $c, c' \in \mathbb{C}$  と任意の  $u \in V$  に対して,  $(cc')u = c(c'u)$  が成り立つ.

ベクトル空間  $V$  のアーベル群としての単位元を **零ベクトル** といい,  $0_V$  (または単に  $0$ ) で表す. ベクトル空間  $V$  の元を **ベクトル** と呼ぶ. 複素数  $c_1, c_2, \dots, c_n \in \mathbb{C}$  と  $V$  の元  $v_1, v_2, \dots, v_n \in V$  を用いて

$$c_1 v_1 + \dots + c_n v_n$$

と表される  $V$  の元を,  $v_1, v_2, \dots, v_n \in V$  の **線型結合** という. ベクトル  $v_1, v_2, \dots, v_n \in V$  が **一次独立** であるとは,  $c_1 v_1 + \dots + c_n v_n = 0_V$  であるのは,  $c_1 = c_2 = \dots = c_n = 0$  のときに限るときをいう. ベクトルの集合  $\{v_1, v_2, \dots, v_n\} \subset V$  が  $V$  の **基底** であるとは, 以下の 2 条件を満たすときをいう.

- (B1) ベクトル  $v_1, v_2, \dots, v_n \in V$  が一次独立である.
- (B2) 任意の  $v \in V$  はベクトル  $v_1, v_2, \dots, v_n \in V$  の線型結合の形で表すことができる.

線形代数の一般論により,  $V$  の基底を構成する一次独立なベクトルの個数は一定であり, この個数を  $V$  の **次元** という. 従って, 次元の個数だけある一次独立なベクトルは自動的に基底となる.

**例 3-1** 複素数成分を持つような  $n$  次正方行列全体  $\text{Mat}_n(\mathbb{C})$  は行列の和とスカラー倍で  $\mathbb{C}$  上のベクトル空間である. 行列  $E_{ij}$  を  $(i, j)$  成分のみが 1 で他が 0 であるような行列とすれば,  $\{E_{ij} \mid 1 \leq i, j \leq n\}$  が  $\text{Mat}_n(\mathbb{C})$  の基底をなす. これを示してみよう.  $E_{ij}$  ( $1 \leq i, j \leq n$ ) が一次独立であることを示すために

$$c_{11}E_{11} + c_{12}E_{12} + \cdots + c_{ij}E_{ij} + \cdots + c_{nn}E_{nn} = O$$

とおく. ここで,  $c_{ij} \in \mathbb{C}$  であり,  $O$  は零行列である. 左辺は  $(c_{ij})_{1 \leq i, j \leq n}$  なので, 全ての  $i, j$  に対して  $c_{ij} = 0$  を得る. よって,  $E_{ij}$  ( $1 \leq i, j \leq n$ ) が一次独立である. 次に, 任意に  $A = (a_{ij})_{1 \leq i, j \leq n}$  をとれば,

$$a_{11}E_{11} + a_{12}E_{12} + \cdots + a_{ij}E_{ij} + \cdots + a_{nn}E_{nn} = A$$

だから, 任意の  $\text{Mat}_n(\mathbb{C})$  の元が  $E_{ij}$  ( $1 \leq i, j \leq n$ ) の線型結合でかける. 以上で  $\{E_{ij} \mid 1 \leq i, j \leq n\}$  が  $\text{Mat}_n(\mathbb{C})$  の基底をなす.

**レポート 3-1** 有限集合  $S$  の各元  $s \in S$  に対して, 写像  $f_s : S \rightarrow \mathbb{C}$  を

$$f_s(t) = \begin{cases} 1 & (t = s) \\ 0 & (t \neq s) \end{cases}$$

によって定める.

- (1)  $S$  から  $\mathbb{C}$  への写像全体  $\text{Map}(S, \mathbb{C})$  は  $\mathbb{C}$  上のベクトル空間であることを示せ.
- (2)  $\{f_s \mid s \in S\}$  は  $\text{Map}(S, \mathbb{C})$  の基底であることを示せ.

**定義 3.7.**  $V$  を  $\mathbb{C}$  上のベクトル空間とする. 写像

$$\langle -, - \rangle : V \times V \rightarrow \mathbb{C}$$

が以下の条件を満たすとき,  $\langle -, - \rangle$  を  $V$  上の **エルミート内積**<sup>\*1</sup> と呼ぶ.

- (HIP1) 任意の  $x, y \in V$  に対して,  $\langle x, y \rangle = \overline{\langle y, x \rangle}$ .
- (HIP2) 任意の  $x, x', y \in V$  に対して,  $\langle x + x', y \rangle = \langle x, y \rangle + \langle x', y \rangle$ .
- (HIP3) 任意の  $x, y \in V$  と, 任意の  $c \in \mathbb{C}$  に対して,  $\langle cx, y \rangle = c \langle x, y \rangle$ .
- (HIP4) 任意の  $x \in V$  に対して,  $\langle x, x \rangle \geq 0$  であり,  $\langle x, x \rangle = 0$  であることと  $x = 0_V$  であることは同値である.

ベクトル空間  $\text{Map}(S, \mathbb{C})$  には, 次のようなエルミート内積が定義される.

$$\langle f, g \rangle := \frac{1}{|S|} \sum_{s \in S} f(s) \overline{g(s)}$$

これがエルミート内積になっていることは直接確認できる. 例えば, 任意の  $f, g \in \text{Map}(S, \mathbb{C})$  に対して,

$$\langle f, g \rangle = \frac{1}{|S|} \sum_{s \in S} f(s) \overline{g(s)} = \frac{1}{|S|} \sum_{s \in S} \overline{g(s)} f(s) = \overline{\frac{1}{|S|} \sum_{s \in S} g(s) \overline{f(s)}} = \overline{\langle g, f \rangle}$$

だから (HIP1) が成り立つ.

**レポート 3-2** ベクトル空間  $\text{Map}(S, \mathbb{C})$  上に定義された

$$\langle f, g \rangle = \frac{1}{|S|} \sum_{s \in S} f(s) \overline{g(s)}$$

\*1 エルミート内積の英訳は Hermitian inner product である.

が, (HIP2)~(HIP4) を満たすことを確認することで, これがエルミート内積となっていることを確認せよ.

$S$  として有限アーベル群  $G$  として,  $\chi, \chi' \in \widehat{G}$  をとれば

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)} = \delta_{\chi, \chi'}$$

と表せる. ここで最右辺の  $\delta_{\chi, \chi'}$  は Kronecker のデルタである.

**補題 3.8.** 指標群  $\widehat{G} \subset \text{Map}(G, \mathbb{C})$  はベクトル空間  $\text{Map}(G, \mathbb{C})$  の基底をなす.

**証明.** 便宜上,  $\widehat{G} = \{\chi_1, \dots, \chi_m\}$  としておく. ベクトル空間  $\text{Map}(G, \mathbb{C})$  の次元は  $|G|$  であることに注意しよう. **定理 3.4** によって,  $|G| = |\widehat{G}|$  であるから,  $\chi_1, \dots, \chi_m$  が一次独立であることを示せば十分である.  $c_1, \dots, c_m \in \mathbb{C}$  として,  $c_1\chi_1 + \dots + c_m\chi_m = 0$  と仮定する. ここで, 右辺は零写像  $0: G \rightarrow \mathbb{C}$  である. このとき,  $c_1\chi_1 + \dots + c_m\chi_m$  と  $\chi_i$  とのエルミート内積をとれば

$$\langle c_1\chi_1 + \dots + c_m\chi_m, \chi_i \rangle = \sum_{j=1}^m c_j \langle \chi_j, \chi_i \rangle = c_i$$

である. 一方,

$$\langle c_1\chi_1 + \dots + c_m\chi_m, \chi_i \rangle = \langle 0, \chi_i \rangle = 0$$

だから  $c_i = 0$  を得る. これを  $i = 1, 2, \dots, m$  で行えば,  $c_1 = c_2 = \dots = c_m = 0$  を得るので,  $\chi_1, \dots, \chi_m$  は一次独立である.  $\square$

**補題 3.8** によって, 任意の  $f \in \text{Map}(G, \mathbb{C})$  は  $G$  の指標  $\chi_1, \dots, \chi_m$  と複素数  $c_1, \dots, c_m$  を用いて

$$f = c_1\chi_1 + c_2\chi_2 + \dots + c_m\chi_m$$

という形で書ける. このとき,  $\chi_i$  とのエルミート内積を計算すれば

$$\langle f, \chi_i \rangle = \langle c_1\chi_1 + c_2\chi_2 + \dots + c_m\chi_m, \chi_i \rangle = c_i$$

となるので, 次のことがわかった.

**定理 3.9.** 有限アーベル群  $G$  の指標群  $\widehat{G}$  は  $\text{Map}(G, \mathbb{C})$  の基底<sup>\*2</sup>をなし, 任意の  $f \in \text{Map}(G, \mathbb{C})$  は

$$f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi$$

と表せる.

<sup>\*2</sup> もっと強く, 正規直交基底をなす