

Chowla の定理について

東大 教養学部 藤崎源二郎

S. Chowla [3] は次の定理を証明した.

定理 p , $p \equiv 3 \pmod{4}$, を素数とすると,
 $\cot(\pi a/p); a = 1, \dots, (p-1)/2$

は有理数体 $\mathbb{Q}$ 上 1 次独立である.

この定理の別証明, 一般化が Ayoub [1], [2], Hassel [4], Iwasawa [5], Okada [6] により与えられている.

ここでは, 上の定理と関連して, 次の定理がなりたつことを述べる.

定理 m を $(m, \varphi(m)) = 1$ であるような奇数とする.

次の (1) ~ (6) はすべて互いに同値である.

(1) $\cot(\pi a/m); 1 \leq a < m/2, (a, m) = 1$

は $\mathbb{Q}$ 上 1 次独立である.

(1') c を $(c, m) = 1$ である整数としてこれを固定する

とき (とくに $C=2$)

$$\cot(C\pi a/m); 1 \leq a < m/2, (a, m)=1$$

は $\mathbb{Q}$ 上 1 次独立である.

(2) m を法として定義される任意の Dirichlet 指標 χ , $\chi(-1) = -1$, に対して

$$\sum_{a=1}^{m-1} \chi(a) a \neq 0.$$

(3) $\tan(\pi a/m); 1 \leq a < m/2, (a, m)=1$ は $\mathbb{Q}$ 上 1 次独立である.

(3') C を $(C, m)=1$ である整数としてこれを固定するとき (とくに $C=2$)

$$\tan(C\pi a/m); 1 \leq a < m/2, (a, m)=1$$

は $\mathbb{Q}$ 上 1 次独立である.

(4) m を法として定義される任意の Dirichlet 指標 χ , $\chi(-1) = -1$, に対して

$$\sum_{a=1}^{m-1} (-1)^a \chi(a) \neq 0.$$

(5) $\sin(2\pi/m)$ が $\cot(2\pi a/m); 1 \leq a < m/2, (a, m)=1$, の有理係数の 1 次結合として表される.

(6) $\sin(2\pi/m)$ が $\tan(2\pi a/m); 1 \leq a < m/2, (a, m)=1$, の有理係数の 1 次結合として表される.

とくに, $m = p$ が奇素数のときには, 上の (1) - (6) はさらに次の (7), (8) に同値である.

(7) $(p-1)/2$ 次の行列

$$A = (2\overline{ab^{-1}} - p)$$

は正則行列である. ここで, $c = \overline{ab^{-1}} \Leftrightarrow a \equiv bc \pmod{p}$,
かつ $1 \leq c < p$, であり, $a = 1, \dots, (p-1)/2$ が行,
 $b = 1, \dots, (p-1)/2$ が列を表す.

(8) $(p-1)/2$ 次の行列

$$B = ((-1)^{\overline{ab^{-1}}})$$

は正則行列である. ここで, $\overline{ab^{-1}}$ の意味は上に述べたとおりであり, $a = 1, \dots, (p-1)/2$ が行, $b = 1, \dots, (p-1)/2$ が列を表す.

文 献

- [1] R. Ayoub: On a theorem of S. Chowla, J. Number Theory, 7 (1975), 105-107.
- [2] R. Ayoub: On a theorem of Iwasawa, J. Number Theory, 7 (1975), 108-120.
- [3] S. Chowla: The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, J. Number Theory, 2 (1970), 120-123

[4] H. Hasse: On a question of S. Chowla, *Acta Arith.* 18 (1971), 275-280

[5] K. Iwasawa: On a theorem of Chowla, 未発表.

[6] T. Okada: On a theorem of S. Chowla, *Hokkaido Math. J.* 6 (1977), 66-68.

文献[6]は, 数理研における講演後に森田康夫氏に教えていただいた.