代数学 C NO.12 要約

今日のテーマ ユークリッドの互除法

例題 12.1. 群 G の元 a が、$a^{1485} = e$, $a^{1716} = e$ をみたすとするとき、$a^{33} = e$ であることを証明しなさい。

(**解答**)

$$e = a^{1716-1485} = a^{231}$$

1485 を 231 でわると商は 6, あまりは 99 であるから、

$$e = a^{1485-231\cdot 6} = a^{99}$$

同様に、231 を 99 でわると商は 2, あまりは 33 であるから、

$$e = a^{231-99\cdot 2} = a^{33} \quad \square$$

さて、$a^{1485} = e_1, a^{1716} = e_2$ とおき、e_1, e_2 が e とは異なるとしてみる。上と全く同じ操作を行なうと、

$$a^{231} = e_2 e_1^{-1}$$

$$a^{99} = e_1(e_2 e_1^{-1})^{-6} = e_1^7 e_2^{-6}$$

$$a^{33} = e_2 e_1^{-1}(e_1^7 e_2^{-6})^{-2} = e_1^{-15} e_2^{13}$$

このことから

$$-15 \cdot 1485 + 13 \cdot 1716 = 33$$

を得る。逆に、この等式さえ知っておれば、上の例題に対する一行の解答が

$$a^{33} = a^{1485\cdot(-15)+1716\cdot 13} = (a^{1485})^{-15}(a^{1716})^{13} = e$$

と言う具合に書ける。

このような計算を容易に行なうのがユークリッドの互除法である。ここでは手っ取り早く、つぎのような行列算を使う方法を紹介する。

例題 12.2 (ユークリッドの互除法). 等式

$$72l + 56m = 8$$

を満たす整数 l, m の組を一組求めよ。

(**解答**) **まず次のような計算を行なう**

$72 \div 56 = 1$ **余り** 16	$72 = 56 \times 1 + 16$	$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 56 \\ 16 \end{pmatrix}$
$56 \div 16 = 3$ **余り** 8	$56 = 16 \times 3 + 8$	$\begin{pmatrix} 56 \\ 16 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 16 \\ 8 \end{pmatrix}$
$16 \div 8 = 2$ **余り** 0	$16 = 8 \times 2 + 0$	$\begin{pmatrix} 16 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$

各々の行の行列算を組み合わせると、

$$\begin{pmatrix} 72 \\ 56 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix}$$

を得る。この式の右辺に現れる正方行列はすべて $M_2(\mathbb{Z})$ の元として可逆であることに注意して、上の式を次のように変形することが出来る。

$$\begin{aligned}\begin{pmatrix}8\\0\end{pmatrix} &= \begin{pmatrix}2&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}3&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}1&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}72\\56\end{pmatrix}\\ &= \begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}72\\56\end{pmatrix} = \begin{pmatrix}-3&4\\7&9\end{pmatrix}\begin{pmatrix}72\\56\end{pmatrix}\end{aligned}$$

この式の第一行に着目すると、$8 = (-3)\times 72 + 4\times 56$ を得る。
(答)　$l = -3, m = 4.$

※レポート問題

(I) $\mathbb{Z}$ の部分群で、$67773, 144381$ で生成されるもの H を

$$H = n\mathbb{Z}$$

の形で書きなさい。(n を求めなさい。)