

# 体の乗法群の有限部分群について

電波通信

2018 年 8 月 1 日

この文章では体  $K$  の乗法群  $K^\times$  の有限部分群が巡回群であることを示す。この文章ではわかりやすさのために自然数の整除関係を  $\preceq$  と書くことにする。つまり  $n$  が  $m$  の約数の時に  $n \preceq m$  と書くのである。 $\leq$  と  $\preceq$  の違いに注意せよ。また、この文書において体とは可換体を指すことに注意せよ。

**定義 1.** 群  $G$  の元  $a$  の位数  $\text{ord}(a)$  を  $a^n = e$  となる最小の  $n$  として定義する。このような  $n$  が存在しない場合には  $\text{ord}(a) = \infty$  とする。

**命題 2.** 群  $G$  の元  $a$  について  $\text{ord}(a) = n = xy$  とすると

$$\text{ord}(a^x) = y$$

となる。

証明. まず、 $(a^x)^y = a^{xy} = e$  なので、 $y \preceq \text{ord}(a^x)$  である。そして、 $a^{x \cdot \text{ord}(a^x)} = (a^x)^{\text{ord}(a^x)} = e$  なので  $x \cdot \text{ord}(a^x) \preceq n$  となる。以上から  $y \preceq \text{ord}(a^x) \preceq y$  なので  $y = \text{ord}(a^x)$  である。  $\square$

準備のために次の整数に関する簡単な補題を証明する。

**補題 3.** 自然数  $n, m$  に対して  $x, y, s, t$  が存在して  $n = sx$ 、 $m = ty$ 、 $\gcd(x, y) = 1$ 、 $xy = \text{lcm}(n, m)$  を充す。

証明. 自然数  $n, m$  に対して  $k$  個の素数  $p_1, p_2, \dots, p_k$  と  $a_1, a_2, \dots, a_k \in \mathbb{Z}_{\geq 0}$  と  $b_1, b_2, \dots, b_k \in \mathbb{Z}_{\geq 0}$  が存在して

$$\begin{aligned} n &= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \\ m &= p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \end{aligned}$$

と書ける。このとき

$$\text{lcm}(n, m) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}$$

である。

$$c_i = \begin{cases} a_i & a_i = \max\{a_i, b_i\} \text{ のとき} \\ 0 & \text{その他} \end{cases}$$

とし

$$d_i = c_i - x_i$$

と定義する。そして

$$e_i = \begin{cases} b_i & b_i > a_i \text{ のとき} \\ 0 & \text{その他} \end{cases}$$

で

$$f_i = b_i - z_i$$

とする。そして

$$\begin{aligned}x &= p_1^{c_1} \cdots p_1^{c_2} \cdots p_k^{c_k} \\s &= p_1^{d_1} \cdots p_2^{d_2} \cdots p_k^{d_k} \\y &= p_1^{e_1} \cdots p_2^{e_2} \cdots p_k^{e_k} \\t &= p_1^{f_1} \cdots p_2^{f_2} \cdots p_k^{f_k}\end{aligned}$$

と定義すると、明らかに  $n = sx$ 、 $m = ty$ 、 $\gcd(x, y) = 1$  を満たし、また、定義から

$$xy = (p_1^{c_1} \cdots p_1^{c_2} \cdots p_k^{c_k})(p_1^{e_1} \cdots p_2^{e_2} \cdots p_k^{e_k}) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)} = \text{lcm}(n, m)$$

を充す。 □

**定理 4.** 群  $G$  の元  $a, b$  は  $ab = ba$  を充し、 $\text{ord}(a) = n$ 、 $\text{ord}(b) = m$  とし、 $l = \text{lcm}(n, m)$  とする。この時  $c \in G$  が存在して

$$\text{ord}(c) = l$$

となる。

証明. まず  $\gcd(n, m) = 1$  の時、 $c = ab$  とおき、 $r = \text{ord}(c)$  とおくと  $l = nm$  よりと  $a$  と  $b$  の可換性より

$$c^l = a^l b^l = ee = e$$

なので  $r \leq l$  でありまた

$$e = c^{nr} = a^{nr} b^{nr} = eb^{nr} = b^{nr}$$

より  $m \leq nr$  ところで  $n, m$  は互いに素なので  $m \leq r$  となる。同様に  $n \leq r$  もわかるので結局  $l \leq r$  (最小公倍数の性質である。) よって  $\text{ord}(c) = l$

一般の場合は  $n = sx$ 、 $m = ty$ 、 $\gcd(x, y) = 1$   $xy = l$  と表せるので  $a^s$  と  $b^t$  を上の場合に当てはめれば結論が得られる。 □

**注意.** また非可換な二元については定理 4 は成り立たないことに注意せよ。例えば三次の対称群などを考えよ。

定理 4 をアーベル群に適用すると次のことがわかる。

**系 5.** 有限可換群  $G$  の元の  $\leq$  に関する最大値を  $N$  とすると、これは  $G$  の元が取りうる位数の中で  $\leq$  に関しても最大値となっている。つまり有限可換群  $G$  のある元  $x$  が存在して

$$\forall a \in G \text{ ord}(a) \leq \text{ord}(x)$$

となるということである。

証明. 上の定理を  $G$  の元に次々に適用すればわかる。 □

**定理 6.** 体  $K$  の乗法群  $K^\times$  の有限部分群は巡回群

証明.  $G$  を  $K^\times$  の有限部分群とする。 $G$  の最大位数を持つ元を  $a$  とし、 $\text{ord}(a) = N$  と置く。 $G$  の任意の元  $s$  について  $\text{ord}(s) \leq N$  なので

$$s^N = 1$$

となる。つまり  $G$  の任意の元は  $K$  上の多項式  $x^N - 1$  の根である。 $x^N - 1$  の根の個数は高々  $N$  個なので

$$|G| \leq N$$

である。ところで  $N \leq |G|$  でもあるから  $N = |G|$  よって  $a$  は  $G$  を生成する。つまり  $G$  は巡回群。  $\square$