次の定理を証明したい.

$\boxed{\text{定理}}$ (可換な)体 K の乗法群 $K^\times$ の有限部分群 G は巡回群になる.

$\boxed{\text{証明 1}}$ (有限生成 Abel 群の基本定理を使う方法)

G は有限 Abel 群なので有限生成 Abel 群の基本定理より,

$$G \cong C_N \times C_{N_1} \times \cdots \times C_{N_r}, \quad N_r | N_{r-1} | \cdots | N_1 | N, \quad N, N_i \in \mathbb{Z}_{>0}$$

と書ける. ここで, C_n は位数 n の巡回群を表す. このとき, $|G| = N N_1 \cdots N_r \geqq N$.

$N_1, \ldots, N_r$ がすべて N の約数になっていることより,

G の任意の元の位数が N の約数になっていることがわかる.

ゆえに任意の $a \in G$ について $a^N = 1$. すなわち, $G \subset \{a \in K \mid a^N = 1\}$.

K は体なので $x^N - 1$ の K に含まれる根の個数は N 以下である.

したがって, $|G| \leqq |\{a \in K \mid a^N = 1\}| \leqq N$.

$|G| \geqq N$ でもあったので $|G| = N$.

これは $G \cong C_N$ を意味する. □

$\boxed{\text{証明2}}$ (初等的な証明)

$N=|G|$ とおく。G が位数 N の元を含むことを示せばよい。
そのためには，$a\in G$ の位数 m が N より小さいならば，a から位数が a より大きな G の元を作れることを示せば十分である。

$a\in G$ の位数 m は N より小さいと仮定する。

$\langle a\rangle$ の位数は m であり，$\langle a\rangle$ の元の m 乗はどれも 1 になる。
K は体なので K に含まれる x^m-1 の根の個数は m 以下である。
ゆえに，$\langle a\rangle=\{x\in K \mid x^m=1\}$。

$m<N$ より $\langle a\rangle\subsetneq G$ となるので，ある $b\in G\setminus\langle a\rangle$ が存在する。

b の位数 n は，$b\notin\langle a\rangle=\{x\in K\mid x^m=1\}$ より，m の約数ではない。

$m=nm'$ ならば
$b^m=b^{nm'}=1$,
$\therefore\ b\in\langle a\rangle$
で矛盾する。

a の位数 m と b の位数 n の最大公約数を g と書き，$c=b^g$ とおく。
n は g で割り切れるが，n は m の約数ではないので $n>g$。
c の位数は $\dfrac{n}{g}>1$ になり，$\dfrac{n}{g}$ と m の最大公約数は 1 になる。
このことから，ac の位数が $m\dfrac{n}{g}>m$ となることがわかる。 □

次ページで示す。

上の証明の最後で次を使った.

$\boxed{\text{補題}}$ Gは群であるとし, $a, b \in G$は互いに可換であると仮定する.

aの位数mとbの位数nの最大公約数が1ならばabの位数はmnになる.

$\boxed{\text{証明}}$ (本質的に中国式剰余定理)

abの位数をlと書く.

$(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$より, lはmnの約数になる.

mとnの最大公約数は1なので, ある$r, s \in \mathbb{Z}$が存在して$rm+sn=1$. ← Euclidの互除法

このとき,

$$(ab)^{sn} = a^{\overbrace{sn}^{1-rm}} \overbrace{b^{sn}}^{1} = a^{1-rm} \overset{a^m=1}{=} a, \quad (ab)^{rm} = \overbrace{a^{rm}}^{1} b^{\overbrace{rm}^{1-sn}} = b^{1-sn} \overset{b^n=1}{=} b.$$

ゆえに,

$$a^l = ((ab)^{sn})^l = (\overbrace{(ab)^l}^{1})^{sn} = 1, \quad b^l = ((ab)^{rm})^l = (\overbrace{(ab)^l}^{1})^{rm} = 1.$$

したがって, lはmとnで割り切れる.

以上を合わせると, $l = mn$が得られる. $\square$

定理の主な応用

空気のごとく使われる!

① 位数 q の有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q^\times$ は位数 $q-1$ の巡回群になる.

$\boxed{例}$ $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0,1,2,3,4\}$ と書くとき,

$\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ と書かずに $0,1,2,3,4$ と書いた. (てぬき!)

$\underline{2} \neq 1,\ 2^2 = \underline{4} \neq 1,\ 2^3 = \underline{3} \neq 1,\ 2^4 = \underline{1}$ より, $\mathbb{F}_5^\times = \langle 2 \rangle$.

$\boxed{例}$ $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{0,1,2,\dots,6\}$ と書くとき,

$\underline{2} \neq 1,\ 2^2 = \underline{4} \neq 1,\ 2^3 = \underline{1}$ なので $\mathbb{F}_7^\times \neq \langle 2 \rangle$,

$\underline{3} \neq 1,\ 3^2 = \underline{2} \neq 1,\ 3^3 = \underline{6} \neq 1,\ 3^4 = \underline{4} \neq 1,\ 3^5 = \underline{5} \neq 1,\ 3^6 = \underline{1}$ より, $\mathbb{F}_7^\times = \langle 3 \rangle$.

$\boxed{例}$ $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{0,1,\omega,1+\omega\}$, $\omega = \bar{x}$ と書くとき,

$\underline{\omega} \neq 1,\ \omega^2 = -\omega - 1 = \underline{1+\omega},\ \omega^3 = \omega + \omega^2 = \omega + 1 + \omega = \underline{1}$ より, $\mathbb{F}_4^\times = \langle \omega \rangle$.

② 任意の体 K と正の整数 n について, $\{x \in K \mid x^n = 1\}$ も巡回群になる.