§9. やり残した証明

● まず，§7 で述べた次の補題の証明を完成させよう．

補題 7.3　A を有限アーベル群とする *(*乗法群とし単位元を 1 で表す*)*．任意の自然数 n に対して $x^n = 1$ をみたす $x \in A$ の個数が n 以下ならば，A は巡回群である．

補題 9.1　A を有限アーベル群とする．$a \in A$ の位数が mn ならば，a^m の位数は n である．

補題 9.2　A を有限アーベル群とし，$a, b \in A$ の位数をそれぞれ m, n とする．m, n が互いに素ならば，ab の位数は mn である．

これら 2 つの補題の証明は演習問題とし，これらを認めて補題 7.3 を証明する．

補題 7.3 の証明　a を A に属する最大位数の元とし，その位数を m とすると，

$$\langle a \rangle = \left\{1, a, a^2, \ldots, a^m - 1\right\}$$

であり，これに属する m 個の元は $x^m = 1$ をみたす．いま，A が巡回群でないと仮定すると，$\langle a \rangle \subsetneq A$，したがって $b \notin \langle a \rangle$ である $b \in A$ がとれる．b の位数を n とするとき，もし $n|m$ が成り立てば，$b^m = 1$ となるから，少なくとも $m+1$ 個の元が $x^m = 1$ をみたし，補題の対偶が得られ，証明は完了する．

そこで，以下で $n|m$ を示す．そのために，任意の素数 p をひとつとって固定し，

$$m = p^e k, \qquad n = p^f l, \qquad kl \not\equiv 0 \pmod{p}$$

のような整数 $e, f \geq 0$ および自然数 k, l をとる（素因数分解の一意性によって，これらは一意にとれる）．補題 9.1 より，a^{p^e} の位数は k であり，b^l の位数は p^f であるが，$p \nmid k$ だから，補題 9.2 より $a^{p^e} b^l$ の位数は $p^f k$ となる．ここで，a の位数 $m = p^e k$ は最大だったから，$p^f k \leq m = p^e k$，したがって $f \leq e$ を得る．任意の素数 p についてこの不等式が成り立つことは，$n|m$ を示している．　(証明終)

● 次の目標は，§8 で述べた次の定理の証明である．

定理 8.2　R を PID とし，K をその商体とする． $f \in R[X]$ に対して，f が K 上の既約多項式 (すなわち $K[X]$ において既約多項式) であるためには，f が R 上の既約多項式 (すなわち $R[X]$ において既約多項式) であることが必要十分である．

商体については（その正確な定義を §5 で述べたが）講義では扱わなかった． ここでは，体 K がその部分整域 R に対して

$$K = \left\{ \frac{b}{a} \;\middle|\; a, b \in R,\ a \neq 0 \right\}$$

をみたすとき，K は R の商体であるということにする． たとえば $\mathbb{Q}$ は $\mathbb{Z}$ の商体であり，$\mathbb{Q}[\sqrt{-1}]$ は $\mathbb{Z}[\sqrt{-1}]$ の商体である．

定理の証明のために，以下の定義と 3 つの補題を用意する（なお，以下では多項式であることを明示するために，f の代わりに $f(X)$ と書くことが多い）．

定義　　可換環 R 上の多項式

$$f(X) = \sum_{k=0}^{n} a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

に対して，R のイデアル $(a_0, \cdots, a_n)$ が (1) であるとき，$f(X)$ は**原始的**であるという．

補題 9.3 (ガウス)　可換環 R 上の 2 つの原始的な多項式 $f(X), g(X)$ の積 $f(X)g(X)$ は原始的である．

補題 9.4　R を整域とし，K をその商体とする． $a, b \in K^\times$ および R 上の 2 つの原始的な多項式 $f(X), g(X)$ が，$af(X) = bg(X)$ をみたすならば，b/a は R の単元である（すなわち，ある $u \in R^\times$ が存在して $f(X) = ug(X)$ が成り立つ）．

補題 9.5　R を PID とすると，任意の $f(X) \in R[X]$ に対して，

$$f(X) = af_1(X)$$

をみたす $a \in R$ および原始的な多項式 $f_1(X) \in R[X]$ が存在する．

これら 3 つの補題は後で証明することにし，一旦これらを認めて定理 8.2 を証明しよう．

定理 8.2 の証明　R 上可約ならば，あきらかに K 上可約なので，以下においては，その逆を示すことにする． いま，$f(X) \in R[X]$ が K 上可約であるとする． すなわち，

$$f(X) = g(X)h(X), \qquad 0 < \deg g(X),\ \deg h(X) < \deg f(X)$$

のような $g(X), h(X) \in K[X]$ が存在する． $g(X)$ の係数は K の元だから，それらを R の元の商で表し，

$$g(X) = \sum_{k=0}^{n} t_k X^k, \qquad t_k = \frac{r_k}{s_k} \quad (r_k, s_k \in R,\ \ k = 0, \ldots, n)$$

とし，$b = s_0 s_1 \cdots s_n$ とおけば $b \neq 0$ かつ $bg(X) \in R[X]$ となる． よって，補題 9.5 より $b_1 \in R$ および原始的な $g_1(X) \in R[X]$ がとれて

$$bg(X) = b_1 g_1(X)$$

と表すことができる． 同様にして，0 でない $c, c_1 \in R$ と原始的な $h_1(X) \in R[X]$ が存在して

$$ch(X) = c_1 h_1(X)$$

と表される． 一方，$f(X)$ はもともと R 上の多項式だから，やはり補題 9.5 を用いて

$$f(X) = af_1(X)$$

をみたす $a \in R$ および原始的な $f_1(X) \in R[X]$ が存在する． よって，

$$af_1(X) = f(X) = g(X)h(X) = \frac{b_1 c_1}{bc} g_1(X)h_1(X)$$

であるが，補題 9.3 より $g_1(X)h_1(X)$ は原始的であり，したがって，補題 9.4 から，

$$f_1(X) = ug_1(X)h_1(X)$$

をみたす $u \in R^\times$ がとれる． すなわち，

$$f(X) = af_1(X) = (aug_1(X))h_1(X)$$

であるが，$aug_1(X), h_1(X)$ はともに R 上の多項式であるから，このことは，$f(X)$ が R 上可約であることを示している． (証明終)

補題 9.3 の証明　f, g および $h = fg$ がそれぞれ

$$f = \sum_{i=0}^{l} a_i X^i, \quad g = \sum_{j=0}^{m} b_j X^j, \quad h = \sum_{k=0}^{n} c_k X^k \qquad (a_i, b_j, c_k \in R)$$

で与えられているとする．もし，h が原始的でないとすると，$(c_0, \ldots, c_n) \subsetneq (1)$ だから，命題 4-3 より，$(c_0, \ldots, c_n) \subset M$ をみたす極大イデアル M がとれる．この M に対して，自然な全射準同型

$$R \longrightarrow R/M, \quad a \mapsto \bar{a}$$

を係数にほどこすことにより，多項式環の準同型

$$R[X] \longrightarrow (R/M)[X], \quad F \mapsto \bar{F}$$

が定義できる．いまの場合，$c_k \in M$ より，R/M において $\bar{c}_k = 0$ だから，

$$\bar{h} = \sum_{k=0}^{n} \bar{c}_k X^k = 0$$

となっている．よって $\bar{f}\bar{g} = 0$ である．ところで，R/M は体なのでその上の多項式環 $(R/M)[X]$ は整域である．よって $\bar{f} = 0$ または $\bar{g} = 0$，言い換えれば $(a_0, \ldots, a_l) \subset M$ または $(b_0, \ldots, b_m) \subset M$ が成り立つ．このことは，f または g が原始的でないことを意味し，仮定に反する．　(証明終)

補題 9.4 の証明　仮定より f, g の次数は等しく，それぞれ

$$f = \sum_{k=0}^{n} a_k X^k, \qquad g = \sum_{l=0}^{n} b_l X^l \qquad (a_k, b_l \in R)$$

で与えられていれば，ともに原始的なので，$(a_0, \ldots, a_n) = (b_0, \ldots, b_n) = (1)$ である．いま，$a, b \in K^\times$ を R の元の商で表し，

$$a = \frac{q}{r}, \quad b = \frac{s}{t} \qquad (q, r, s, t \in R)$$

とすると，仮定 $af = bg$ は，$qtf = rsg$ と書き換えることができるから，はじめから $a, b \in R$ であるとして証明すればよい．そこで，イデアルの 2 つの等式

$$(a) = (a)(1) = (a)(a_0, \ldots, a_n) = (aa_0, \ldots, aa_n),$$
$$(b) = (b)(1) = (b)(b_0, \ldots, b_n) = (bb_0, \ldots, bb_n)$$

を考えると，それぞれの最右辺は等しいので，$(a) = (b)$ であり，(R が整域であることから) ある $u \in R^\times$ がとれて $b = au$ と表される．よって，$f = (b/a)g = ug$ を得る．　(証明終)

補題 9.5 の証明　f が

$$f = \sum_{i=0}^{m} a_i X^i \qquad (a_i \in R)$$

で与えられているとする．R が PID なので，

$$(a_0, a_1, \ldots, a_m) = (c)$$

をみたす $c \in R$ が存在する．$f \neq 0$ としてよいから，$c \neq 0$ である．さらに，$a_i \in (c)$ だから，$a_i = b_i c$ をみたす $b_i \in R$ が各 i に対してとれる．そこで，

$$f_1 = \sum_{i=0}^{m} b_i X^i$$

とおくと $f = cf_1$ である．さらに f_1 は原始的である．実際，$(b_0, b_1, \ldots, b_m) = (d)$ をみたす $d \in R$ をとれば，

$$(c) = (a_0, a_1, \ldots, a_m) = (b_0 c, b_1 c, \ldots, b_m c) = (c)(b_0, b_1, \ldots, b_m) = (c)(d) = (cd)$$

だから，$cd = cu$ をみたす $u \in R^\times$ が存在するが，$c \neq 0$ より $d = u \in R^\times$ となるから，$(b_0, b_1, \ldots, b_m) = (d) = (1)$ を得る．　(証明終)