代数学概論 B 演習

黒木玄 2008 年 6 月 23 日 (月) (教師用)

目 次

5 一意分解整域 (続き)

5.1 一意分解整域の定義

以下 R は (可換な) 整域であるとする.

定義 5.1 (素元と既約元)

- $p \in R$ が R の**素元**であるとは $p \neq 0$ かつ p で生成される単項イデアル $(p) = Rp$ が R の素イデアルになることである. $0 \neq p \in R$ のとき, p が R の既約元であることと $a, b \in R$, $p \mid ab$ ならば $p \mid a$ または $p \mid b$ となることは同値である.
- $p \in R$ が R の**既約元**であるとは p が非可逆でかつ $p = ab$, $a, b \in R$ ならば a または b が可逆になることである. たとえば 1 は可逆なので既約元ではなく, $0 = 0 \cdot 0$ で 0 は非可逆なので 0 は既約元ではない. □

注意 5.2 永尾の教科書 [1] では上の意味での既約元を素元と呼んでいる. □

定義 5.3 (同伴) R における同値関係 $\approx$ を次のように定める: $a, b \in R$ に対して

$$a \approx b \iff R \text{ の可逆元 } u \text{ で } a = ub \text{ を満たすものが存在する.}$$

$a \approx b$ が成立するとき a と b は**同伴**であると言う. □

R は整域なので $(a) = (b)$ と $a \approx b$ は同値になる. R の素元 (もしくは既約元) と同伴な元もまた素元 (もしくは既約元) になる.

定義 5.4 (一意分解整域, UFD) R が**一意分解整域 (unique factorization domain, UFD)** であるとは R が (可換な) 整域でかつ以下の条件を満たしていることである:

(a) **既約元分解の存在:** $a \in R$ が 0 でない非可逆元ならば R の既約元 $p_1, p_2, \ldots, p_r$ が存在して $a = p_1 p_2 \cdots p_r$ が成立する.

(b) **既約元分解の一意性:** $p_1, \ldots, p_r, q_1, \ldots, q_s$ が R の既約元で $p_1 \cdots p_r = q_1 \cdots q_s$ ならば $r = s$ であり, 適当に番号を付け変えれば $p_i \approx q_i$ $(i = 1, \ldots, r)$ となる. □

注意 5.5 上の定義は永尾 [1], p.101 の「一意分解環」の定義と一致している. ただし永尾が素元と呼んでいるものがここでは既約元と呼ばれていることに注意せよ. □

5.2 既約元の完全代表系

R は一意分解整域であるとする.

R の既約元の全体を同伴という同値関係で同値類に類別したときの完全代表系 $\mathcal{P}$ と書く. すなわち $\mathcal{P}$ は R の既約元の集合であり, 以下の二つの条件を満たしているとする:

(A) R の任意の既約元 p に対してある $q \in \mathcal{P}$ が存在して $p \approx q$.

(B) 任意の $p, q \in \mathcal{P}$ に対して $p \approx q$ ならば $p = q$.

このような $\mathcal{P}$ の存在は選択公理を使って証明される. 詳しくは同値関係による類別について詳しく解説している任意の教科書を参照せよ. $\mathcal{P}$ を**既約元の完全代表系**と呼ぶことにする.

定理 5.6 このとき以下が成立している:

(1) 任意の 0 でない $a \in R$ に対して R の可逆元 u と互いに異なる $p_1, \ldots, p_r \in \mathcal{P}$ と正の整数 $e_1, \ldots, e_r$ で次を満たすものが存在する:

$$a = u p_1^{e_1} \cdots p_r^{e_r}.$$

(2) このような u は a から一意に定まり, $(p_1, e_1), \ldots, (p_r, e_r)$ は並べる順序を除いて a から一意に定まる.

証明. (1) a が可逆元ならば $u = a$ とおけばよい. R は一意分解整域なので条件 (a) より a が非可逆ならば R の既約元 $q_1, \ldots, q_s$ が存在して $a = q_1 \cdots q_s$ が成立する. $\mathcal{P}$ は既約元の完全代表系なので条件 (A) より各 $i = 1, \ldots, s$ ごとにある $p_i \in \mathcal{P}$ が存在して $q_i \approx p_i'$ となる. すなわち R の可逆元 u_i が存在して $q_i = u_i p_i'$ となる. $u = u_1 \cdots u_s$ とおく. u は R の可逆元である. $p_1', \ldots, p_s'$ の中に現われる $\mathcal{P}$ の互いに異なる元の全体を $p_1, \ldots, p_r$ と書き, $p_1', \ldots, p_s'$ の中に現われる p_i の個数を e_i と書く. このとき

$$a = q_1 \cdots q_s = (u_1 p_1') \cdots (u_s p_s') = u p_1^{e_1} \cdots p_r^{e_r}.$$

これで (1) が証明された.

(2) u, v は R の可逆元であり, $p_1, \ldots, p_r, q_1, \ldots, q_s \in \mathcal{P}$ であり, $p_1, \ldots, p_r$ は互いに異なり, $q_1, \ldots, q_s$ も互いに異なるものとし, $e_1, \ldots, e_r, f_1, \ldots, f_s$ は正の整数であり, $u p_1^{e_1} \cdots p_r^{e_r} = v q_1^{f_1} \cdots q_r^{f_r}$ であると仮定する. $u = v$ でかつ $r = s$ で適当に番号を付け変えれば $p_i = q_i$, $e_i = f_i$ $(i = 1, \ldots, r)$ となることを示せばよい.

以下 $p \in \mathcal{P}$ を含む同伴に関する同値類を $[p]$ と表わす. $\mathcal{P}$ は既約元の完全代表系なので条件 (B) より $p, q \in \mathcal{P}$ に対して $p \approx q$ と $p = q$ は同値になる.

$u p_1$, $v q_1$ も R の既約元であり, $u p_1 \approx p_1$, $v q_1 \approx q_1$ でかつ

$$\underbrace{(u p_1) p_1 \cdots p_1}_{e_1} \cdots \underbrace{p_r \cdots p_r}_{e_r} = \underbrace{(v q_1) q_1 \cdots q_1}_{f_1} \cdots \underbrace{q_s \cdots q_s}_{f_s}.$$

R は一意分解整域なので条件 (b) より, $(\underbrace{q_1, \ldots, q_1}_{f_1}, \ldots, \underbrace{q_s, \ldots, q_s}_{f_s})$ を適当に並び換えて $(\underbrace{p_1, \ldots, p_1}_{e_1}, \ldots, \underbrace{p_r, \ldots, p_r}_{e_r})$ に等しくなるようにできる. $p_1, \ldots, p_r$ は互いに異なり, $q_1, \ldots, q_s$ も互いに異なり, e_i, f_j は正の整数なので $r = s$ でかつ適当に番号を付け変えることによって $p_i = q_i$, $e_i = f_i$ $(i = 1, \ldots, r)$ が成立する.

このとき $p_1^{e_1} \cdots p_r^{e_r} = q_1^{f_1} \cdots q_r^{f_r}$ が成立するので R が整域であることより $u = v$ が成立することもわかる. (整域では一般に $uk = vk$, $k \neq 0$ ならば $u = v$ が成立する.)

以上によって (2) も証明された. □

5.3 一意分解整域における最大公約元と最小公倍元

定義 5.7 (最大公約元, 最小公倍元) R は整域であるとし, $a,b \in R$ であるとする.

- $d \in R$ が a,b の**公約元**であるとは $d \mid a$ かつ $d \mid b$ が成立することである.
- a,b の公約元 g が a,b の**最大公約元**であるとは a,b の任意の公約元 d に対して $d \mid g$ が成立することである.
- $m \in R$ が a,b の**公倍元**であるとは $a \mid m$ かつ $a \mid m$ が成立することである.
- a,b の公倍元 l が a,b の**最小公倍元**であるとは a,b の任意の公倍元 m に対して $l \mid m$ が成立することである. □

以下 R は一意分解整域であるとし, $\mathcal{P}$ は R の既約元の完全代表系であるとする.

補題 5.8 一意分解整域 R において 0 でない $a,b \in R$ に対して, R の可逆元 u,v と互いに異なる $p_1,\dots,p_r$ と **0 以上の**整数 e_i, f_i $(i=1,\dots,r)$ が存在して

$$a = up_1^{e_1}\cdots p_r^{e_r}, \quad b = vp_1^{f_1}\cdots p_r^{f_r}. \tag{$*$}$$

証明. 定理 5.6 (1) より, $a \neq 0$ に対して R の可逆元 u と互いに異なる $p_1,\dots,p_s \in \mathcal{P}$ と正の整数 $e_1,\dots,e_s$ が存在して $a = up_1^{e_1}\cdots p_s^{e_s}$ となる. 同様に $b \neq 0$ に対して R の可逆元 v と互いに異なる $p_{s+1},\dots,p_r \in \mathcal{P} - \{p_1,\dots,p_s\}$ と 0 以上の整数 $f_1,\dots,f_r$ が存在して $b = vp_1^{f_1}\cdots p_r^{f_r}$ となる. $e_{s+1} = \cdots = e_r = 0$ とおけば $a = up_1^{e_1}\cdots p_r^{e_r}$ が成立する. □

補題 5.9 u,v は R の可逆元であり, $p_1,\dots,p_r \in \mathcal{P}$ は互いに異なり, e_i, f_i $(i=1,\dots,r)$ は **0 以上の**整数であり, $up_1^{e_1}\dots p_r^{e_r} = vp_1^{f_1}\cdots p_r^{f_r}$ ならば $u=v$ かつ $e_i = f_i$ $(i=1,\dots,r)$ が成立する.

証明. $e_i \neq 0$ となる i の全体を $1 \leqq i_1 < \cdots < i_s \leqq r$ と書き, $f_j \neq 0$ となる j の全体を $1 \leqq j_1 < \cdots < j_t \leqq r$ と書くと $up_{i_1}^{e_{i_1}}\cdots p_{i_s}^{e_{i_s}} = vp_{j_1}^{f_{j_1}}\cdots p_{j_t}^{f_{j_t}}$ が成立する. 定理 5.6 (2) より $u=v$, $s=t$, $i_\nu = j_\nu$, $e_{i_\nu} = f_{j_\nu}$ $(\nu = 1,\dots,s)$ が成立しなければいけない. $i_1,\dots,i_s$ 以外の i について $e_i = 0 = f_i$ が成立している. □

定理 5.10 一意分解整域 R において 0 でない a,b を補題 5.8 の $(*)$ のように表わしておく. このとき以下が成立している:

(i) $a \mid b \iff e_i \leqq f_i$ $(i=1,\dots,r)$.

(ii) $g = p_1^{d_1}\cdots p_r^{d_r}$, $d_i = \min\{e_i, f_i\}$, $l = p_1^{m_1}\cdots p_r^{m_r}$, $m_i = \max\{e_i, f_i\}$ とおくと g,l はそれぞれ a,b の最大公約元, 最大公倍元である.

証明. (i) の $\Longleftarrow$. $e_i \leqq f_i$ $(i=1,\dots,r)$ のとき $c = (vu^{-1})p_1^{f_1-e_1}\cdots p_r^{f_r-e_r}$ とおくと $ac = b$ なので $a \mid b$ である.

(i) の $\Longrightarrow$. $a \mid b$ ならばある $c \in R$ が存在して $ac = b$ となる. $b \neq 0$ より $c \neq 0$ である. 補題 5.8 の証明と同様にして R の可逆元 w と互いに異なる $p_{r+1},\dots,p_t \in \mathcal{P} - \{p_1,\dots,p_r\}$ と 0 以上の整数 $g_1,\dots,g_t$ が存在して $c = wp_1^{g_1}\cdots p_t^{g_t}$ となる. このとき $ac = b$ より $(uw)p_1^{e_1+g_1}\cdots p_r^{e_r+g_r}p_{r+1}^{g_{r+1}}\cdots p_t^{g_t} = vp_1^{f_1}\cdots p_r^{f_r}p_{r+1}^0\cdots p_t^0$ となる. 補題 5.9 より $uw = v$, $e_i + g_i = f_i$ $(i=1,\dots,r)$, $g_j = 0$ (j=r+1,...,t) となる. 特に $e_i \leqq f_i$ $(i=1,\dots,r)$.

ここで次を示しておこう:

- a, b の任意の公約元 d は次のように表わされる:

$$d = wp_1^{c_1} \cdots p_r^{c_r}, \quad w \text{ は } R \text{ の可逆元}, \quad 0 \leqq c_i \leqq \min\{e_i, f_i\} \quad (i = 1, \ldots, r).$$

- a, b の任意の 0 でない公約元 m は次のように表わされる:

$$m = zp_1^{n_1} \cdots p_r^{n_r}, \quad z \in R, \quad \max\{e_i, f_i\} \leqq n_i \quad (i = 1, \ldots, r).$$

$m = 0$ なら $z = 0, n_i = \max e_i, f_i$ とおけばよい. そこで以下では $m \neq 0$ と仮定する. 補題 5.8 の証明と同様にして R の可逆元 w, y と互いに異なる $p_{r+1}, \ldots, p_t \in \mathcal{P} - \{p_1, \ldots, p_r\}$ と 0 以上の整数 c_i, n_i $(i = 1, \ldots, t)$ が存在して $d = wp_1^{c_1} \cdots p_t^{c_t}$, $m = yp_1^{n_1} \cdots p_t^{n_t}$ となる. (i) の $\Longrightarrow$ より $c_i \leqq \min\{e_i, f_i\}$ $(i = 1, \ldots, r)$, $c_j = 0$ $(j = r+1, \ldots, t)$, $\max\{e_i, f_i\} \leqq n_i$ $(i = 1, \ldots, r)$, $0 \leqq n_j$ $(j = r+1, \ldots, t)$ となることがわかる. 特に $d = wp_1^{c_1} \cdots p_r^{c_r}$ が成立しており, $z = yp_{r+1}^{n_{r+1}} \cdots p_t^{n_t}$ とおけば $m = zp_1^{n_1} \cdots p_r^{n_r}$ も成立している.

(ii) (i) の $\Longleftarrow$ より g, l がそれぞれ a, b の公約元, 公倍元であることがわかる. d, m はそれぞれ a, b の公約元, 公倍元であると仮定し, 上のようにそれらを表わしておく. このとき (i) の $\Longleftarrow$ より $d \mid g$, $l \mid m$ となることがわかる. これで g, l がそれぞれ a, b の最大公約元, 最小公倍元であることが示された. □

5.4 まとめ

以上の結果を用いて次の定理を証明できる.

定理 5.11 R は一意分解整域であり, R の商体を K と書く. $\mathcal{P}$ は R の既約元の完全代表系であるとする. R, K の可逆元全体の集合をそれぞれ $R^\times$, $K^\times$ と書き, 群 $\mathbb{Z}^{\oplus\mathcal{P}}$ を次のように定める:

$$\mathbb{Z}^{\oplus\mathcal{P}} = \{\, (e_p)_{p\in\mathcal{P}} \mid e_p \in \mathbb{Z} \text{ であり, 有限個を除いて } e_p = 0 \,\}.$$

このとき次の写像は群の同型写像である:

$$\varphi : R^\times \times \mathbb{Z}^{\oplus\mathcal{P}} \xrightarrow{\sim} K^\times, \quad (u, (e_p)_{p\in\mathcal{P}}) \mapsto u \prod_{p\in\mathcal{P}} p^{e_p}.$$

有限個を除いて $e_p = 0$ なので $\prod_{p\in\mathcal{P}} p^{e_p}$ は有限積になることに注意せよ. □

問題 5.12 (研究課題) 上の定理を証明せよ. さらに $R = \mathbb{Z}, k[x]$ (k は任意の体) の場合に $R^\times$ がどうなるかを示し, 既約元の完全代表系 $\mathcal{P}$ の例を挙げ, 同型写像 φ を記述せよ. □

参考文献

[1] 永尾汎, 代数学, 新数学講座 4, 朝倉書店, 1983