1　ねじれ加群

R を可換環とし, 0_R を R の零元, 1_R を R の単位元とする. また, M を R 加群とし, 0_M を M の零元とする.

M の元 x が自由元であるとは, 任意の $r \in R$ に対して,

$$rx = 0_M \Longrightarrow r = 0_R$$

が成り立つときにいう. M の元 x が自由元であることと, x が R 上 1 次独立であることは同じ意味である.

M の元 x がねじれ元であるとは, 自由元でないときにいう. すなわち, ある $r \in R$ が存在して

$$rx = 0_M, \quad r \neq 0_R$$

が成り立つとき, x はねじれ元であるという. M の零元 0_M はねじれ元である. 実際, $1_R \cdot 0_M = 0_M$ である.

[定理 1.1] R を整域, M を R 加群とする. このとき, M のねじれ元全体からなる集合 $T(M)$ は M の部分 R 加群である. $T(M)$ を M のねじれ部分という.

[証明] まず, $0_M \in T(M)$ であるから, $T(M) \neq \emptyset$.

$x, y \in T(M), r \in R$ を任意にとる. x はねじれ元であるから, ある $r_1 \in R$ が存在して, $r_1 x = 0_M$ かつ $r_1 \neq 0_R$. 同様に, y はねじれ元であるから, ある $r_2 \in R$ が存在して, $r_2 y = 0_M$ かつ $r_2 \neq 0_R$. このとき, R の可換性により,

$$\begin{aligned} r_1 r_2 (x + y) &= r_1 r_2 x + r_1 r_2 y \\ &= r_2 (r_1 x) + r_1 (r_2 y) \\ &= 0_M. \end{aligned}$$

しかも, R は零因子をもたないから, $r_1 r_2 \neq 0_R$. ゆえに, $x + y \in T(M)$. さらに, R の可換性により,

$$r_1 (rx) = r(r_1 x) = 0_M.$$

ゆえに, $rx \in T(M)$. したがって, $T(M)$ は M の部分 R 加群である. $\square$

[定理 1.2] R を整域, M, M' を R 加群, $f : M \to M'$ を R 準同型とする. このとき,

$$f\bigl(T(M)\bigr) \subseteq T\bigl(f(M)\bigr)$$

が成り立つ. さらに, f が単射ならば, 等号が成り立つ.

［**証明**］ $x \in T(M)$ を任意にとる. ある $r \in R$ が存在して,

$$rx = 0_M, \quad r \neq 0_R.$$

f の準同型性より,

$$r \cdot f(x) = f(rx) = f(0_M) = 0_{M'}.$$

ゆえに, $f\bigl(T(M)\bigr) \subseteq T\bigl(f(M)\bigr)$.

次に, f が単射であると仮定する. $y \in f\bigl(T(M)\bigr)$ とすると, ある $r \in R$ が存在して,

$$ry = 0_{M'}, \quad r \neq 0_R.$$

$y \in f(M)$ であるから, ある $x \in M$ が存在して, $y = f(x)$. よって,

$$f(rx) = r \cdot f(x) = ry = 0_{M'}.$$

f の単射性より, $rx = 0_M$. ゆえに, $x \in T(M)$. したがって, $y \in f\bigl(T(M)\bigr)$ となり, 逆の包含関係もいえる. □

以下, R を整域, M を R 加群とする.

M のすべての元がねじれ元であるとき, すなわち $M = T(M)$ であるとき, M はねじれ加群であるという. 特に, M のねじれ部分 $T(M)$ は常にねじれ加群である.

M が 0_M 以外にねじれ元をもたないとき, すなわち $T(M) = \{0_M\}$ であるとき, M はねじれがないという.

［**定理 1.3**］ R を整域, M を R 加群とする. このとき, 剰余 R 加群 $M/T(M)$ はねじれがない.

［**証明**］ $\pi : M \to M/T(M)$ を自然な全射 R 準同型とする.

$T(M) = M$ のとき. $M/T(M) = \{0_{M/T(M)}\}$ となり, 明らかにねじれがない.

$T(M) \subsetneq M$ のとき. $x \in M \setminus T(M)$, $r \in R$ とし,

$$r \cdot \pi(x) = 0_{M/T(M)}$$

と仮定する.

$$\begin{aligned} r \cdot \pi(x) &= 0_{M/T(M)} \\ &\Longrightarrow \pi(rx) = 0_{M/T(M)} \\ &\Longrightarrow rx \in T(M) \end{aligned}$$

であるから, ある $s \in R$ が存在して,

$$srx = 0_M, \quad s \neq 0_R.$$

$x \notin T(M)$, すなわち x は M の自由元であるから, $sr = 0_R$. さらに, R は零因子をもたないから, $r = 0_R$ でなければならない. したがって, $\pi(x)$ は $M/T(M)$ の自由元である. □

[定理 1.4] 整域上の自由加群はねじれがない.

[証明] R を整域, M を自由 R 加群とし, $B = \{u_i \mid i \in I\}$ (I は添字集合) を M の R 上の基底とする.

$x \in T(M)$ とすると, ある $r \in R$ が存在して,

$$rx = 0_M, \quad r \neq 0_R.$$

B は M の R 上の生成系だから,

$$x = \sum_{j=1}^{s} a_j u_j,$$

$$a_j \in R, \quad u_j \in B$$

と表せる. よって,

$$\sum_{j=1}^{s} r a_j u_j = rx = 0_M.$$

$u_1, u_2, \ldots, u_s$ は R 上 1 次独立だから, すべての $j = 1, 2, \ldots, s$ に対して,

$$r a_j = 0_R.$$

さらに, $r \neq 0_R$ であり, かつ R は零因子をもたないから, すべての $j = 1, 2, \ldots, s$ に対して,

$$a_j = 0_R.$$

ゆえに, $x = 0_M$. したがって, $T(M) \subseteq \{0_M\}$. 逆の包含関係は明らかだから, $T(M) = \{0_M\}$. すなわち, M はねじれがない. □

[定理 1.5] R を単項イデアル整域とする. このとき, ねじれがない有限生成 R 加群は階数有限の自由 R 加群である.

[証明] M をねじれがない有限生成 R 加群とすると, $T(M) = \{0_M\}$ である. $M = \{0_M\}$ のときは定理は明らかに成り立つので, $M \neq \{0_M\}$ であるとする. そのとき, M は, ある有限個の 0_M でない元 $x_1, x_2, \ldots, x_n \in M$ によって R 上生成される. M はねじれがないから, $x_1, x_2, \ldots, x_n$ の各々は自由元である.

R は Noether 環だから, M は Noether 加群である. M の部分自由 R 加群で階数有限のものからなる集合を $\mathcal{M}$ とおく. 例えば Rx_1 は M の階数有限の部分自由 R 加群であるから, $\mathcal{M} \neq \emptyset$ である. よって, $\mathcal{M}$ は極大元 N をもつ.

各 $i = 1, 2, \ldots, n$ に対して, ある $r_i \in R$ が存在して, $r_i x_i \in N$ かつ $r_i \neq 0_R$ となる. なぜなら, もし仮にそうでないとすると, ある番号 i_0 が存在して, 任意の $r \in R$ に対して,

$$r x_{i_0} \in N \Longrightarrow r = 0_R$$

である. $v_1, v_2, \ldots, v_k$ を N の生成元とすると, 任意の $r_1, r_2, \ldots, r_k, r \in R$ に対して,

$$\begin{aligned}
\left(\sum_{j=1}^{k} r_j v_j\right) + r x_{i_0} = 0_M \\
&\Longrightarrow r x_{i_0} = -\sum_{j=1}^{k} r_j v_j \in N \\
&\Longrightarrow r = 0_R, \sum_{j=1}^{k} r_j v_j = 0_M \\
&\Longrightarrow r = r_1 = \cdots = r_k = 0_R.
\end{aligned}$$

よって, $v_1, v_2, \ldots, v_k, x_{i_0}$ は R 上 1 次独立である. このとき, 集合 $\{v_1, v_2, \ldots, v_k, x_{i_0}\}$ は M の部分 R 加群 $N + Rx_{i_0}$ の R 上の基底である. ゆえに, $N + Rx_{i_0}$ は M の部分自由 R 加群となり, かつ $N \subsetneq N + Rx_{i_0}$ となる. これは N の極大性に反する.

さて, 写像

$$\begin{aligned}
f : M &\to N, \\
x &\mapsto (r_1 r_2 \cdots r_n) x
\end{aligned}$$

を考える. f は R 準同型である. また,

$$\ker f \subseteq T(M) = \{0_M\}$$

より, $\ker f = \{0_M\}$ であるから, f は単射である. よって, $M \cong f(M)$ となる. さらに, $f(M)$ は N の部分 R 加群であるが, R は単項イデアル整域なので, $f(M)$ もまた階数有限の自由 R 加群である. ゆえに, M も階数有限の自由 R 加群である. □

［系 1.6］ R を単項イデアル整域とし, M を有限生成 R 加群, $T(M)$ を M のねじれ部分とする. このとき, 剰余 R 加群 $M/T(M)$ は階数有限の自由 R 加群である.

［証明］ 定理 1.3, 定理 1.5 より明らかである. □

［補題 1.7］ R を可換環, M, N を R 加群, $f : N \to M$, $g : M \to N$ を R 準同型とし,

$$g \circ f = \mathrm{id}_N$$

であるとする. このとき, f は単射, g は全射であって,

$$\begin{aligned}
M &= \ker g \oplus f(N) \\
&\cong \ker g \oplus N
\end{aligned}$$

が成り立つ.

［証明］$g \circ f = \mathrm{id}_N$ より, f は単射, g は全射である.
$x \in M$ を任意にとる.

$$z = x - f(g(x)) \in M$$

とおけば,

$$g(z) = g(x) - g(f(g(x))) = 0_N.$$

ゆえに,

$$\begin{aligned} x &= z + f(g(x)) \\ &\in \ker g \oplus f(N). \end{aligned}$$

また, $x \in \ker g \cap f(N)$ とすると, ある $y \in N$ が存在して, $x = f(y)$. このとき,

$$y = g(f(y)) = g(x) = 0_N.$$

よって,

$$x = g(0_N) = 0_M.$$

ゆえに,

$$\ker g \cap f(N) = \{0_M\}.$$

以上より,

$$M = \ker g \oplus f(N).$$

さらに, f の単射性より $N \cong f(N)$ だから,

$$\ker g \oplus f(N) \cong \ker g \oplus N$$

も成り立つ. □

［補題 1.8］R を可換環, M を R 加群, L を階数有限の自由 R 加群とし, $g : M \to L$ を全射 R 準同型とする. このとき, ある単射 R 準同型 $f : L \to M$ が存在して,

$$g \circ f = \mathrm{id}_L$$

かつ

$$M \cong \ker g \oplus L$$

が成り立つ.

［証明］$\{u_1, u_2, \ldots, u_n\}$ を L の R 上の基底とする. すべての $y \in L$ は,

$$y = \sum_{i=1}^{n} r_i u_i, \quad r_i \in R$$

の形に一意的に表される. また, g は全射だから, 各 $i = 1, 2, \ldots, n$ に対して, ある $x_i \in M$ が存在して, $g(x_i) = u_i$ となる. そこで, 写像 $f : L \to M$ を

$$f(y) = \sum_{i=1}^{n} r_i x_i$$

により定める. f は R 準同型である. また, $g \circ f = \mathrm{id}_L$ が成り立ち, f は単射である. またこのとき, 補題 1.7 より, R 同型 $M \cong \ker g \oplus L$ が得られる. □

［定理 1.9］ R を単項イデアル整域とし, M を有限生成 R 加群, $T(M)$ を M のねじれ部分とする. このとき,

$$M \cong T(M) \oplus \bigl(M/T(M)\bigr)$$

が成り立つ.

［証明］ 自然な全射 R 準同型 $M \to M/T(M)$ の核は $T(M)$ である. 系 1.6 より $M/T(M)$ は自由 R 加群だから, 補題 1.8 より求める同型が得られる. □

2 零化域

可換環 R 上の加群 M の元 x に対して,

$$\mathrm{Ann}_R(x) = \{r \in R \mid rx = 0_M\}$$

を x の零化域という. R 自身を R 加群とみなしたとき, $\mathrm{Ann}_R(x)$ は, R 加群の準同型

$$R \to M, \quad r \mapsto rx$$

の核である. よって, $\mathrm{Ann}_R(x)$ は R の部分 R 加群であり, それはまさに R のイデアルである.

$\mathrm{Ann}_R(x)$ が R の零イデアルであることと, x が M の自由元であることは同値である. また, $\mathrm{Ann}_R(x) = R$ であることは, $x = 0_M$ であることと同値である.

R が単項イデアル整域のとき, $\mathrm{Ann}_R(x)$ は R の単項イデアルであり, ある 1 個の元によって生成される.

［定理 2.1］ R を単項イデアル整域, M を R 加群, x を M の元, p を R の素元とする. このとき, 次の 2 条件は同値である.

(i) ある整数 $e \geq 0$ が存在して, $\mathrm{Ann}_R(x) = p^e R$.

(ii) ある整数 $e \geq 0$ が存在して, $p^e x = 0_M$.

［**証明**］(i)⇒(ii)　$\mathrm{Ann}_R(x)$ の生成元が p の冪と同伴であるとすると, ある整数 $e \geq 0$ が存在して,

$$\mathrm{Ann}_R(x) = p^e R$$

が成り立つ. 特に, $p^e \in \mathrm{Ann}_R(x)$ であるから, $p^e x = 0_M$ となる.

(ii)⇒(i)　ある整数 $e \geq 0$ が存在して, $p^e x = 0_M$ であると仮定する. $e = 0$ のとき, $x = 0_M$ であり, $\mathrm{Ann}_R(x)$ の生成元は 1_R である. $e > 0$ のとき, $\mathrm{Ann}_R(x)$ の生成元を a とおくと,

$$p^e \in \mathrm{Ann}_R(x) = aR.$$

すなわち, ある $b \in R$ が存在して,

$$p^e = ab.$$

R は素元分解整域であり, p は素元であるから, 素元分解の一意性より, a は p の冪と同伴でなければならない. □

［**定理 2.2**］R を単項イデアル整域, M を巡回 R 加群, x を M の生成元, a を $\mathrm{Ann}_R(x)$ の生成元とする. このとき, R 加群としての同型

$$M \cong R/aR$$

が成り立つ. さらに, M が自由 R 加群かつ $M \neq \{0_M\}$ であれば, M は R 加群として R と同型である.

［**証明**］M は x を生成元とする巡回 R 加群なので, $M = Rx$ である. このとき, R 加群としての準同型

$$R \to M, \quad r \mapsto rx$$

は全射であり, その核は $\mathrm{Ann}_R(x)$ であるから, 準同型定理により

$$R/\mathrm{Ann}_R(x) \cong M.$$

a は $\mathrm{Ann}_R(x)$ の生成元だから, $\mathrm{Ann}_R(x) = aR$. ゆえに, $R/aR \cong M$.

M が巡回自由 R 加群であるとすると, 一般に単項イデアル整域上の自由加群はねじれがないから, M はねじれがない. また, $M \neq \{0_M\}$ ならば $x \neq 0_M$ である. よって, x は自由元であり, $a = 0_R$ である. したがって, $R \cong M$ となる. □

R を単項イデアル整域とし, M を R 加群とする. M と, R の素元 p に対して,

$$M(p) = \{x \in M \mid \text{ある整数 } e \geq 0 \text{ が存在して}, p^e x = 0_M\}$$

とおく. $M(p)$ は, ねじれ加群であり, M の部分 R 加群である.

［**定理 2.3**］R を単項イデアル整域, M を R 加群, p, q を R の素元とする.

(i) p, q が互いに素のとき,

$$M(p) \cap M(q) = \{0_M\}.$$

(ii) p, q が同伴のとき,

$$M(p) = M(q).$$

［**証明**］(i)　$x \in M(p) \cap M(q)$ とすると, ある整数 $e \geq 0$, $e' \geq 0$ が存在して,

$$p^e x = q^{e'} x = 0_M.$$

一方, R は単項イデアル整域であり, p, q は互いに素だから, ある r, $s \in R$ が存在して,

$$p^e r + q^{e'} s = 1_R.$$

ゆえに,

$$\begin{aligned} x &= 1_R \cdot x \\ &= (p^e r + q^{e'} s)\, x \\ &= r(p^e x) + s(q^{e'} x) \\ &= 0_M \end{aligned}$$

となる.

(ii)　$x \in M(p)$ とすると, ある整数 $e \geq 0$ が存在して, $p^e x = 0_M$ である. p, q は同伴であるから, R の単元 ε が存在して, $q = p\varepsilon$. このとき,

$$q^e x = (p\varepsilon)^e x = \varepsilon^e (p^e x) = 0_M.$$

よって, $x \in M(q)$. ゆえに, $M(p) \subseteq M(q)$. 逆の包含関係も同様にして示せる. □

［**定理 2.4**］R を単項イデアル整域, M, M' を R 加群, $f : M \to M'$ を R 準同型, p を R の素元とする. このとき,

$$f\big(M(p)\big) \subseteq \big(f(M)\big)(p)$$

が成り立つ. さらに, f が単射ならば, 等号が成り立つ.

［**証明**］$x \in M(p)$ とすると, ある整数 $e \geq 0$ が存在して, $p^e x = 0_M$ である. f の準同型性より,

$$p^e f(x) = f(p^e x) = f(0_M) = 0_{M'}.$$

ゆえに, $f\big(M(p)\big) \subseteq \big(f(M)\big)(p)$.

次に, f が単射であると仮定する. $y \in \bigl(f(M)\bigr)(p)$ とすると, ある整数 $e \geq 0$ が存在して, $p^e y = 0_{M'}$ である. $y \in f(M)$ であるから, ある $x \in M$ が存在して, $y = f(x)$. よって,

$$f(p^e x) = p^e f(x) = p^e y = 0_{M'}.$$

f の単射性より, $p^e x = 0_M$. ゆえに, $x \in M(p)$. したがって, $y \in f\bigl(M(p)\bigr)$ となり, 逆の包含関係もいえる. □

［定理 2.5］ R を単項イデアル整域, M を有限生成ねじれ R 加群とする. このとき, ある素元 $p_1, p_2, \ldots, p_t \in R$ が存在して, 直和分解

$$M = \bigoplus_{i=1}^{t} M(p_i)$$

が成り立つ. しかも, $p_1, p_2, \ldots, p_t$ は互いに同伴でないようにとれる.

［証明］ $u_1, u_2, \ldots, u_k$ を M の R 上の生成元とする. 各 u_i は 0_M でないとしておく.

各 $i = 1, 2, \ldots, k$ に対して, r_i を $\mathrm{Ann}_R(u_i)$ の生成元とする. M はねじれ加群だから, $r_i \neq 0_R$ である. また, $u_i \neq 0_M$ としたから, r_i は単数ではない. R は素元分解整域であり, $r_1 r_2 \cdots r_k$ は R の零元でも単元でもないから, 互いに同伴でない素元 $p_1, p_2, \ldots, p_t$ によって,

$$r_1 r_2 \cdots r_k = \varepsilon' p_1^{e_1'} \cdots p_t^{e_t'}$$

と素元分解される. ただし, ε' は R の単元, $e_i' \geq 1$ は整数である.

さて, $x \in M$ を任意にとる. x は $u_1, u_2, \ldots, u_k$ の R 上の 1 次結合で表される. このとき,

$$(r_1 r_2 \cdots r_k) x = 0_M.$$

すなわち,

$$r_1 r_2 \cdots r_k \in \mathrm{Ann}_R(x).$$

r を $\mathrm{Ann}_R(x)$ の生成元とすると,

$$r \mid r_1 r_2 \cdots r_k.$$

したがって, r は

$$r = \varepsilon p_1^{e_1} \cdots p_t^{e_t}, \quad 0 \leq e_i \leq e_i'$$

の形に素元分解される. ただし, ε は R の単元, e_i は整数である. r の代わりに $r\varepsilon^{-1}$ をとり, $\varepsilon = 1_R$ としてよい. $i = 1, 2, \ldots, t$ に対して

$$q_i = \prod_{1 \leq j \leq t,\, j \neq i} p_i^{e_i}$$

とおけば, $q_1, q_2, \ldots, q_t$ の最大公約元は 1_R であるから,

$$\sum_{i=1}^{n} s_i q_i = 1_R, \quad s_i \in R$$

と表される. このとき,

$$x = 1_R \cdot x = \sum_{i=1}^{n} (s_i q_i x).$$

さらに,

$$p_i^{e_i}(s_i q_i x) = s_i r x = 0_M$$

であるから,

$$s_i q_i x \in M(p_i).$$

ゆえに,

$$M = \sum_{i=1}^{t} M(p_i).$$

次に, $x_i \in M(p_i)$ $(i = 1, 2, \ldots, t)$ とし,

$$\sum_{i=1}^{t} x_i = 0_M$$

と仮定する. 定理 2.1 より, 各 $i = 1, 2, \ldots, t$ に対して, ある整数 $e_i \geq 0$ が存在して,

$$\mathrm{Ann}_R(x_i) = p_i^{e_i} R$$

が成り立つ. i を任意に 1 つ固定したとき,

$$x_i = - \sum_{1 \leq j \leq t,\, j \neq i} x_j,$$

$$q_i x_j = 0_M \ (j \neq i)$$

であるから, $q_i x_i = 0_M$ である. R は単項イデアル整域であり, $p_i^{e_i}$ と q_i は互いに素だから, ある $u, v \in R$ が存在して,

$$p_i^{e_i} u + q_i v = 1_R.$$

ゆえに,

$$\begin{aligned} x_i &= 1_R \cdot x_i \\ &= u(p_i^{e_i} x_i) + v(q_i x_i) \\ &= 0_M. \end{aligned}$$

したがって, M は $M(p_1), M(p_2), \ldots, M(p_t)$ の直和に分解される. $\square$

R を単項イデアル整域, M を R 加群, p を R の素元とする. $M = M(p)$ であるとき, すなわち, 任意の $x \in M$ に対して, ある整数 $e \geq 0$ が存在して $p^e x = 0_M$ が成り立つとき, M を p 加群という. p 加群はねじれ加群である.

［**定理 2.6**］R を単項イデアル整域, p を R の素元, M を有限生成 p 加群とする. このとき, ある整数 $e_1, e_2, \ldots, e_k$ が存在して,

$$M \cong \bigoplus_{i=1}^{k} R/p^{e_i}R$$

かつ

$$1 \leq e_1 \leq e_2 \leq \cdots \leq e_k$$

が成り立つ.

［**証明**］$\mathcal{G}$ を M の R 上の生成系のうち有限集合であるもの全体とし, $\mathcal{G}$ に属する生成系の元の個数の最小値を k とする. $\{x_1, x_2, \ldots, x_k\}$ を k 個の元よりなる生成系とすると, M は p 加群なので, 定理 2.1 より, すべての $i = 1, 2, \ldots, k$ に対して, ある整数 $e_i \geq 0$ が存在して,

$$\mathrm{Ann}_R(x_i) = p^{e_i}R$$

が成り立つ. k 個の元よりなる生成系のうち $\displaystyle\sum_{i=1}^{k} e_i$ が最小であるものを改めて $\{x_1, x_2, \ldots, x_k\}$ とする. 必要ならば, 番号を付け替えて

$$e_1 \leq e_2 \leq \cdots \leq e_k$$

とする. もし仮に $e_1 = 0$ であるとすると, $\mathrm{Ann}_R(x_1) = R$ であるから,

$$x_1 = 1_R \cdot x_1 = 0_M$$

となって, $k-1$ 個の元からなる集合 $\{x_2, \ldots, x_k\}$ が $\mathcal{G}$ に属することになり, k の最小性に反する. ゆえに, $e_1 \geq 1$ である.

さて, M が

$$M = \bigoplus_{i=1}^{k} Rx_i$$

のように直和に分解されることが示せたとする. 各 $i = 1, 2, \ldots, k$ に対して, 定理 2.2 より

$$\begin{aligned} Rx_i &\cong R/\mathrm{Ann}_R(x_i) \\ &= R/p^{e_i}R \end{aligned}$$

である. これにより, 求める R 同型が得られる. 一方, $\{x_1, x_2, \ldots, x_k\}$ は M の R 上の生成系なので,

$$M = \sum_{i=1}^{k} Rx_i.$$

したがって, 各 $i = 1, 2, \ldots, k-1$ に対して

$$\left(\sum_{j=0}^{i-1} Rx_{k-j}\right) \cap Rx_{k-i} = \{0_M\}$$

が成り立つことを証明すれば十分である．これを背理法により示す．

ある i_0 $(1 \leq i_0 \leq k-1)$ が存在して, 上式が $i = 1, 2, \ldots, i_0 - 1$ に対しては成り立つが, $i = i_0$ に対しては成り立たないと仮定する．R の部分集合

$$\mathfrak{a} = \left\{ r \in R \;\middle|\; r x_{k-i_0} \in \sum_{j=0}^{i_0-1} R x_{k-j} \right\}$$

は R のイデアルである．R は単項イデアル整域だから, ある $a_0 \in R$ が存在して, $\mathfrak{a} = a_0 R$ となる．$p^{e_{k-i_0}} \in \mathfrak{a}$ だから, ある $s \in R$ が存在して, $p^{e_{k-i_0}} = a_0 s$ である．R は素元分解整域であり, p は R の素元だから, ある整数 e' が存在して, a_0 は $p^{e'}$ と同伴であり, かつ $0 \leq e' \leq e_{k-i_0}$ である．もし仮に $e' = e_{k-i_0}$ であるとすると, $p^{e'} x_{k-i_0} = 0_M$．ところが, 背理法の仮定より, ある $a \in R$ が存在して,

$$a x_{k-i_0} \in \sum_{j=0}^{i_0-1} R x_{k-j}, \quad a x_{k-i_0} \neq 0_M.$$

1 番目の式より

$$a \in \mathfrak{a} = a_0 R = p^{e'} R$$

であるから, $a x_{k-i_0} = 0_M$．これは 2 番目の式に反する．ゆえに, $e' < e_{k-i_0}$．また,

$$p^{e'} x_{k-i_0} = \sum_{j=0}^{i_0-1} r_j p^{f_j} x_{k-j},$$

$$r_j \in R, \quad f_j \in \mathbb{Z}, \quad f_j \geq 0$$

と表せる．ただし, $r_j \neq 0_R$ ならば $p \nmid r_j$ とする．両辺に $p^{e_{k-i_0} - e'}$ を掛けると,

$$\begin{aligned} 0_M &= p^{e_{k-i_0}} x_{k-i_0} \\ &= \sum_{j=0}^{i_0-1} r_j p^{e_{k-i_0} - e' + f_j} x_{k-j}. \end{aligned}$$

M の部分 R 加群 $N = \displaystyle\sum_{j=0}^{i_0-1} R x_{k-j}$ は, 背理法の仮定より

$$N = \bigoplus_{j=0}^{i_0-1} R x_{k-j}$$

のように直和に分解される．よって, 各 $j = 0, 1, \ldots, i_0 - 1$ に対して,

$$r_j p^{e_{k-i_0} - e' + f_j} x_{k-j} = 0_M,$$

すなわち,

$$r_j p^{e_{k-i_0} - e' + f_j} \in p^{e_{k-j}} R.$$

もし $r_j \neq 0_R$ ならば, $p \nmid r_j$ なので,

$$e_{k-i_0} - e' + f_j \geq e_{k-j},$$

したがって,

$$f_j - e' \geq e_{k-j} - e_{k-i_0} \geq 0.$$

そこで, M の元 x'_1, x'_2, …, x'_k を, $i = k - i_0$ のとき

$$x'_{k-i_0} = x_{k-i_0} - \sum_{j=0}^{i_0-1} r_j p^{f_j - e'} x_{k-j}$$

とおき, それ以外のとき $x'_i = x_i$ とおくことにより定めれば,

$$\{x'_1, x'_2, \ldots, x'_k\} \in \mathcal{G}$$

であり, しかも

$$p^{e'} x'_{k-i_0} = 0_M.$$

定理 2.1 より, 各 $i = 1, 2, \ldots, k$ に対して, ある整数 $e'_i \geq 0$ が存在して,

$$\mathrm{Ann}_R(x'_i) = p^{e'_i} R$$

が成り立つ. このとき, $e'_{k-i_0} \leq e'$ であり, かつ $i \neq k - i_0$ なるすべての番号 i に対しては $e'_i = e_i$ である. したがって,

$$\sum_{i=1}^{k} e'_i \leq e' + \sum_{i \neq k-i_0} e_i < \sum_{i=1}^{k} e_i.$$

これは $\displaystyle\sum_{i=1}^{k} e_i$ の最小性に反する. □

3　単項イデアル整域上の有限生成加群の構造定理

［**定理 3.1**（**単項イデアル整域上の有限生成加群の構造定理**）］ R を単項イデアル整域, M を有限生成 R 加群とする. このとき, R の 2 つずつ同伴でない素元 p_1, p_2, …, p_t と, 整数 $e_{i,j}$ ($i = 1$, 2, …, t; $j = 1$, 2, …, $u(i)$) が存在して,

$$M \cong \left(\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}} R \right) \right) \oplus R^s \tag{1}$$

かつ, 各 $i = 1, 2, \ldots, t$ に対して,

$$1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,u(i)}$$

が成り立つ. しかも, イデアルの列の集合

$$\left\{ \left(p_i^{e_{i,1}} R, \ldots, p_i^{e_{i,u(i)}} R \right) \,\middle|\, i = 1, 2, \ldots, t \right\}$$

および s は, M に対して一意的に定まる.

［**証明**］$T(M)$ を M のねじれ部分とする．定理 1.9 より, R 同型

$$M \cong T(M) \oplus \bigl(M/T(M)\bigr)$$

が成り立つ．系 1.6 より, $M/T(M)$ は階数有限の自由 R 加群である．ゆえに, ある整数 $s \geq 0$ が存在して,

$$M/T(M) \cong R^s.$$

また, 定理 2.5 より, R の 2 つずつ同伴でない素元 $p_1, p_2, \ldots, p_t$ が存在して,

$$T(M) = \bigoplus_{i=1}^{t} \bigl(T(M)\bigr)(p_i).$$

さらに, 各 $i = 1, 2, \ldots, t$ に対して, 定理 2.6 より, 整数 $u(i) \geq 1$ と整数 $e_{i,j}$ が存在して,

$$\bigl(T(M)\bigr)(p_i) \cong \bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}}R$$

かつ,

$$1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,u(i)}.$$

ゆえに, M を式 (1) の形で表すことができる．

次に, 一意性を証明する．M が式 (1) の形で表されると仮定すると, 補題 4.1 (後述) より,

$$\begin{aligned} T(M) &\cong \bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}}R \right), \\ M/T(M) &\cong R^s \end{aligned}$$

が成り立つ．自由加群の階数の一意性により, s は M に対して一意的に定まる．また, イデアルの列の集合 $\{(p_i^{e_{i,j}})\}$ の一意性は補題 4.9 (後述) よりわかる． □

［**系 3.2（有限生成 Abel 群の構造定理）**］G を有限生成 Abel 群とする．このとき, 互いに異なる素数 $p_1, p_2, \ldots, p_t$ と, 整数 $e_{i,j}$ $(i = 1, 2, \ldots, t;\ j = 1, 2, \ldots, u(i))$ が存在して,

$$G \cong \left(\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} \mathbb{Z}/p_i^{e_{i,j}}\mathbb{Z} \right) \right) \oplus \mathbb{Z}^s$$

かつ, 各 $i = 1, 2, \ldots, t$ に対して,

$$1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,u(i)}$$

が成り立つ．しかも, 素数の列の集合

$$\left\{ \bigl(p_i^{e_{i,1}}, \ldots, p_i^{e_{i,u(i)}}\bigr) \;\middle|\; i = 1, 2, \ldots, t \right\}$$

および s は, M に対して一意的に定まる．

［**証明**］Abel 群とは $\mathbb{Z}$ 加群のことである．$R = \mathbb{Z}$ として定理 3.1 を適用すればよい． $\square$

［**定理 3.3（単項イデアル整域上の有限生成加群の構造定理）**］R を単項イデアル整域, M を有限生成 R 加群とする．このとき, R の元 d_1, d_2, …, d_u が存在して,

$$M \cong \left(\bigoplus_{j=1}^{u} R/d_j R \right) \oplus R^s \tag{2}$$

かつ, 各 $i = 1$, 2, …, u に対して,

$$R \neq d_1 R \supseteq d_2 R \supseteq \cdots \supseteq d_u R \neq \{0_M\}$$

が成り立つ．しかも, $d_1 R$, $d_2 R$, …, $d_u R$ および s は M に対して一意的に定まる．

［**証明**］定理 3.1 より, R の 2 つずつ同伴でない素元 p_1, p_2, …, p_t と, 整数 $e_{i,j}$ ($i = 1$, 2, …, t; $j = 1$, 2, …, $u(i)$) が存在して,

$$M \cong \left(\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}} R \right) \right) \oplus R^s$$

かつ, 各 $i = 1$, 2, …, t に対して,

$$1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,u(i)}$$

が成り立つ．そこで,

$$u = \max\{u(i) \mid i = 1,\ 2, \ldots,\ t\}$$

とおき, 各 $i = 1$, 2, …, t に対して,

$$e^*_{i,j} = \begin{cases} 0, & j \leq u - u(i) \text{ のとき}, \\ e_{i,j-u+u(i)}, & j > u - u(i) \text{ のとき} \end{cases}$$

とおく．すると,

$$\begin{aligned} &\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}} R \right) \\ &\quad \cong \bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u} R/p_i^{e^*_{i,j}} R \right) \\ &\quad \cong \bigoplus_{j=1}^{u} \left(\bigoplus_{i=1}^{t} R/p_i^{e^*_{i,j}} R \right). \end{aligned}$$

各 $j = 1$, 2, …, u に対して,

$$d_j = \prod_{i=1}^{t} p_i^{e^*_{i,j}}$$

とおく. $d_u \neq 0_R$ かつ d_1 は R の単元ではなく, すべての $j = 1, 2, \ldots, u-1$ に対して,

$$d_j \mid d_{j+1}.$$

また, $p_1, p_2, \ldots, p_t$ は 2 つずつ互いに素だから, 中国剰余定理により,

$$R/d_jR \cong \bigoplus_{i=1}^{t} R/p_i^{e_{i,j}^*}R.$$

ゆえに,

$$\bigoplus_{i=1}^{t}\left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}}R\right) \cong \bigoplus_{j=1}^{u} R/d_jR.$$

よって, M を式 (2) の形で表すことができる.

次に, 一意性を証明する. 補題 4.1 (後述) より,

$$T(M) \cong \bigoplus_{i=1}^{u} R/d_jR,$$

$$M/T(M) \cong R^s$$

が成り立つ. 自由加群の階数の一意性により, s は M に対して一意的に定まる. また, $d_1, d_2, \ldots, d_u$ のいずれかの素元分解に現れる 2 つずつ互いに素な素元を $p_1, p_2, \ldots, p_t$ とし, 各 $j = 1, 2, \ldots, u$ に対して,

$$d_j = \varepsilon_j \prod_{i=1}^{t} p_i^{e_{i,j}^*}, \quad e_{i,j}^* \geq 0$$

を素元分解とする. ここで, ε_j は R の単元である. d_i についての条件から, 各 $j = 1, 2, \ldots, u$ に対して,

$$0 \leq e_{1,j}^* \leq e_{2,j}^* \leq \cdots \leq e_{t,j}^*$$

であり, 少なくとも 1 つの j に対して $e_{1,j}^* \geq 1$ であり, またすべての j に対して $e_{t,j}^* \geq 1$ である. 各 $i = 1, 2, \ldots, t$ に対して, $e_{i,j}^* = 0$ が成り立つ j の最大値を $u(i)$ とおき, 各 $j = 1, 2, \ldots, u - u(i)$ に対して,

$$e_{i,j} = e_{i,j+u(i)}^*$$

とおく. すると,

$$\begin{aligned}
T(M) &\cong \bigoplus_{j=1}^{u} R/d_jR \\
&\cong \bigoplus_{j=1}^{u}\left(\bigoplus_{i=1}^{t} R/p_i^{e_{i,j}^*}R\right) \\
&\cong \bigoplus_{i=1}^{t}\left(\bigoplus_{j=1}^{u} R/p_i^{e_{i,j}^*}R\right) \\
&\cong \bigoplus_{i=1}^{t}\left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{i,j}}R\right).
\end{aligned}$$

また, 各 $i = 1, 2, \ldots, t$ に対して,

$$1 \leq e_{i,1} \leq e_{i,2} \leq \cdots \leq e_{i,u(i)}$$

が成り立つ. 別の $d_1, d_2, \ldots, d_u$ に対しても, $T(M)$ についての R 同型による同様の表示が得られる. 補題 4.9 (後述) より t, p_iR, $u(i)$, $e_{i,j}$ は一意的である. これより, $e^*_{i,j}$ の一意性がいえる. したがって, $d_1, d_2, \ldots, d_u$ は, 各 $j = 1, 2, \ldots, u$ に対して, 単数倍 ε_j を除いて一致しなければならない. $\square$

［系 3.4（有限生成 Abel 群の構造定理）］ G を有限生成 Abel 群とするとき, 正の整数 d_1, d_2, $\ldots$, d_u が存在して,

$$M \cong \left(\bigoplus_{j=1}^{u} \mathbb{Z}/d_j\mathbb{Z} \right) \oplus \mathbb{Z}^s$$

かつ,

$$d_1 > 1, \quad d_i \mid d_{i+1} \quad (i = 1, 2, \ldots, u-1)$$

が成り立つ. しかも, $d_1, d_2, \ldots, d_u$ および s は M に対して一意的に定まる.

［証明］ Abel 群とは $\mathbb{Z}$ 加群のことである. $R = \mathbb{Z}$ として定理 3.3 を適用すればよい. $\square$

4　構造定理の一意性を示すための補題

　この節では, 単項イデアル整域上の有限生成加群の構造定理における一意性を示すときに使用した補題を証明する.

［補題 4.1］ R を単項イデアル整域, M を R 加群, $T(M)$ を M のねじれ部分とし,

$$M \cong \left(\bigoplus_{i=1}^{r} R/d_iR \right) \oplus R^s$$

であるとする. ただし, $d_1, d_2, \ldots, d_r$ は R の 0 でない元とする. このとき,

$$T(M) \cong \bigoplus_{i=1}^{r} R/d_iR,$$

$$M/T(M) \cong R^s$$

が成り立つ.

［証明］ $N = \displaystyle\bigoplus_{i=1}^{r} R/d_iR$ とおく. R 加群の同型写像

$$f : N \oplus R^s \to M$$

が与えられたとする. N および R^s からの入射

$$\iota_1 : N \to N \oplus R^s,$$
$$\iota_2 : R^s \to N \oplus R^s$$

を考え, $i = 1, 2$ に対して

$$f_i = f \circ \iota_i$$

とおく. すると, M は

$$M = f_1(N) \oplus f_2(R^s)$$

のように直和分解される.

さて, $d = d_1 d_2 \cdots d_r$ とおくと, R は整域なので $d \neq 0_R$. さらに, 任意の $x \in N$ に対して,

$$d \cdot f_1(x) = f_1(dx) = f_1(0_N) = 0_M.$$

ゆえに, $f_1(N) \subseteq T(M)$. もし仮に $f_1(N) \neq T(M)$ とすると, ある $x \in T(M) \setminus f_1(N)$ が存在する. $x \in M$ より

$$x = y + z, \quad y \in f_1(N), \quad z \in f_2(R^s)$$

と表せる. もし仮に $z = 0_M$ とすると $x \notin f_1(N)$ に反するから, $z \neq 0_M$ である. f_2 は単射だから, $f_2^{-1}(z) \in R^s$ かつ $f_2^{-1}(z) \neq 0_{R^s}$ である. また, $z = x - y \in T(M)$ より, ある $a \in R$ が存在して,

$$az = 0_M, \quad a \neq 0_R.$$

よって,

$$a \cdot f_2^{-1}(z) = f_2^{-1}(az) = 0_{R^s}.$$

ゆえに, $(c_1, c_2, \ldots, c_s) = f_2^{-1}(z)$ とおくと,

$$(c_1, c_2, \ldots, c_s) \neq 0_{R^s},$$
$$(ac_1, ac_2, \ldots, ac_s) = 0_{R^s}.$$

1 番目の式より, ある番号 i が存在して $c_i \neq 0_R$. ところが, 2 番目の式より $ac_i = 0_R$ であり, R が整域であることと $a \neq 0_R$ より $c_i = 0_R$. これは矛盾である. ゆえに, $f_1(N) = T(M)$ でなければならない. これにより, R 加群の同型

$$(N \oplus R^s)/\iota_1(N) \cong M/T(M),$$

が成り立つ. さらに, R^s への射影

$$N \oplus R^s \to R^s$$

の核は $\iota_1(N)$ であるから, 準同型定理より R 加群の同型

$$(N \oplus R^s)/\iota_1(N) \cong R^s$$

が得られる．したがって，

$$M/T(M) \cong R^s$$

が成り立つ． $\square$

［**補題 4.2**］R を単項イデアル整域とし，p を R の素元とする．このとき，R 加群としての同型

$$\bigoplus_{i=1}^{u} R/pR \cong \bigoplus_{i=1}^{u'} R/pR$$

が成り立てば，$u = u'$ である．

［**証明**］まず，R 自身は R 加群であり，pR は R の部分 R 加群である．したがって，R/pR は R の pR による剰余 R 加群である．$\pi : R \to R/pR$ を自然な全射 R 準同型とする．$K = R/pR$ とおくと，

$$K^u = \bigoplus_{i=1}^{u} R/pR,$$
$$K^{u'} = \bigoplus_{i=1}^{u'} R/pR$$

である．これらは R 加群である．各 $a \in R$ と $x \in K^u$ に対して，スカラー倍を

$$\pi(a) \cdot x = ax$$

と定めれば，K^u は K 加群になる．同様にして，$K^{u'}$ も K 加群になる．R は単項イデアル整域であるから，

$$\begin{aligned} p \text{ は } R \text{ の素元} &\Longrightarrow pR \text{ は } R \text{ の素イデアル} \\ &\Longrightarrow pR \text{ は } R \text{ の極大イデアル} \\ &\Longrightarrow K = R/pR \text{ は体.} \end{aligned}$$

ゆえに，K^u, $K^{u'}$ は K 上のベクトル空間であり，K 上の次元はそれぞれ u, u' である．さらに，$f : K^u \to K^{u'}$ を R 同型とすると，任意の $a \in R$ と $x \in K^u$ に対して

$$\begin{aligned} f\big(\pi(a) \cdot x\big) &= f(a \cdot x) = a \cdot f(x) \\ &= \pi(a) \cdot f(x) \end{aligned}$$

であるから，f は K 同型でもある．したがって，K^u, $K^{u'}$ の K 上の次元は一致する．すなわち，$u = u'$ となる． $\square$

［**補題 4.3**］R を単項イデアル整域，M を巡回 R 加群，x を M の生成元，a を $\mathrm{Ann}_R(x)$ の生成元とする．このとき，a と互いに素な任意の $b \in R$ に対して，$bM = M$ が成り立つ．

［証明］R は単項イデアル整域であり, a, b は互いに素だから, ある r, $s \in R$ が存在して,

$$1_R = ra + sb.$$

ゆえに,

$$\begin{aligned} x &= (ra + sb)x \\ &= rax + sbx \\ &= b(sx) \in bM. \end{aligned}$$

したがって, $M \subseteq bM$. 逆の包含関係は明らかだから, $bM = M$. □

［補題 4.4］ R を単項イデアル整域, p, q を R の素元, M を巡回 R 加群とする. x を M の R 上の生成元, $e \geq 1$ を整数とし, $\mathrm{Ann}_R(x) = q^e R$ であるとする. さらに, $i \geq 0$ を整数とする.

(i) p, q が互いに素のとき,

$$p^i M / p^{i+1} M \cong \{0_R\}.$$

(ii) p, q が同伴 かつ $e \leq i$ のとき,

$$p^i M / p^{i+1} M \cong \{0_R\}.$$

(iii) p, q が同伴 かつ $e > i$ のとき,

$$p^i M / p^{i+1} M \cong R/pR.$$

［証明］(i)　補題 4.3 より,

$$p^i M = M, \quad p^{i+1} M = M$$

であるから,

$$p^i M / p^{i+1} M = M/M \cong \{0_R\}.$$

(ii)　p, q は同伴だから,

$$\mathrm{Ann}_R(x) = q^e R = p^e R.$$

さらに, $e \leq i$ より,

$$p^i M = \{0_M\}, \quad p^{i+1} M = \{0_M\}.$$

ゆえに,

$$p^i M / p^{i+1} M = \{0_M\}/\{0_M\} \cong \{0_R\}.$$

(iii)　$M = Rx$ より,

$$f : R \to p^i M, \quad r \mapsto p^i(rx)$$

は全射 R 準同型である.

$$\pi_i : p^i M \to p^i M/p^{i+1}M$$

を自然な全射 R 準同型とする. π_i と f との合成

$$\pi_i \circ f : R \to p^i M/p^{i+1}M$$

は全射 R 準同型である. また, $\ker \pi_i \circ f = pR$ である. 実際, $r \in \ker \pi_i \circ f$ とすれば,

$$p^i(rx) = f(r) \in \ker \pi_i = p^{i+1}M.$$

よって, ある $s \in R$ が存在して,

$$p^i(rx) = p^{i+1}(sx).$$

移項すると,

$$p^i(r - ps)x = 0_M.$$

ゆえに,

$$p^i(r - ps) \in \mathrm{Ann}_R(x) = p^e R.$$

R は素元分解整域であり, $e > i$ であるから,

$$r - ps \in p^{e-i}R.$$

ゆえに, $r \in pR$. 逆に, $r \in pR$ とすれば,

$$f(r) = p^i(rx) \in p^{i+1}M$$

となり, $r \in \ker \pi_i \circ f$ である. したがって, $\ker \pi_i \circ f = pR$. 準同型定理により, R 加群の同型

$$R/pR \cong p^i M/p^{i+1}M$$

が得られる. □

[補題 4.5] R を単項イデアル整域とし, p を R の素元とする. このとき, R 加群としての同型

$$\bigoplus_{j=1}^{u} R/p^{e_j}R \cong \bigoplus_{j=1}^{u'} R/p^{e'_j}R$$

が成り立ち, さらに

$$\begin{aligned} &0 < e_1 \leq e_2 \leq \cdots \leq e_u, \\ &0 < e'_1 \leq e'_2 \leq \cdots \leq e'_{u'} \end{aligned} \tag{3}$$

であれば,

$$u = u', \quad e_j = e'_j \quad (j = 1, 2, \ldots, u)$$

となる.

［証明］ $N = \bigoplus_{j=1}^{u} R/p^{e_j}R$, $N' = \bigoplus_{j=1}^{u'} R/p^{e'_j}R$ とおく．$f : N \to N'$ を R 同型とする．

整数 $i \geq 0$ を固定する．まず, $f(p^iN) = p^iN'$ が成り立つから, f の p^iN への制限

$$f_i : p^iN \to p^iN', \quad x \mapsto f(x)$$

は R 同型である．さらに,

$$\begin{aligned} f_i(p^{i+1}N) &= f(p^{i+1}N) = p^{i+1} \cdot f(N) \\ &= p^{i+1}N' \end{aligned}$$

であるから,

$$p^iN/p^{i+1}N \cong p^iN'/p^{i+1}N'.$$

次に,

$$\begin{aligned} p^iN &= p^i \left(\bigoplus_{j=1}^{u} R/p^{e_j}R \right) \\ &= \bigoplus_{j=1}^{u} p^i(R/p^{e_j}R). \end{aligned}$$

補題 4.4 より, $e_j \leq i$ ならば $p^i(R/p^{e_j}R) \cong \{0_R\}$ であるから,

$$\bigoplus_{j=1}^{u} p^i(R/p^{e_j}R) \cong \bigoplus_{e_j > i} p^i(R/p^{e_j}R).$$

よって, R 同型

$$g : p^iN \to \bigoplus_{e_j > i} p^i(R/p^{e_j}R)$$

が存在する．$p^{i+1}N$ は p^iN の部分 R 加群であり,

$$\begin{aligned} g(p^{i+1}N) &= p \cdot g(p^iN) \\ &= p \left(\bigoplus_{e_j > i} p^i(R/p^{e_j}R) \right) \\ &= \bigoplus_{e_j > i} p^{i+1}(R/p^{e_j}R) \end{aligned}$$

であるから,

$$\begin{aligned} p^iN/p^{i+1}N &\cong g(p^iN)/g(p^{i+1}N) \\ &\cong \bigoplus_{e_j > i} \frac{p^i(R/p^{e_j}R)}{p^{i+1}(R/p^{e_j}R)} \\ &\cong \bigoplus_{e_j > i} R/pR. \end{aligned}$$

ここで, 最後の R 同型に補題 4.4 を用いた. 同様にして, R 同型

$$p^i N'/p^{i+1}N' \cong \bigoplus_{e'_j > i} R/pR$$

も得られる. ゆえに, R 同型

$$\bigoplus_{e_j > i} R/pR \cong \bigoplus_{e'_j > i} R/pR$$

が成り立つ.

$$n(i) = \#\{j \mid e_j > i\},$$
$$n'(i) = \#\{j \mid e'_j > i\}$$

とおけば, 補題 4.2 より, $n(i) = n'(i)$ となる.

以上より, 任意の整数 $i \geq 0$ に対して,

$$n(i) = n'(i)$$

が成り立つ. $i = 0$ のとき,

$$u = n(0) = n'(0) = u'.$$

また, 各 $k = 0, 1, 2, \ldots, u-1$ に対して, 条件 (3) と

$$n'(e_{u-k}) = n(e_{u-k}) \leq k$$

より, $e'_{u-k} \leq e_{u-k}$. 逆に, 条件 (3) と

$$n(e_{u-k}) = n(e'_{u-k}) \leq k$$

より, $e_{u-k} \leq e'_{u-k}$. ゆえに, $e_{u-k} = e'_{u-k}$. したがって, すべての $j = 1, 2, \ldots, u$ に対して, $e_j = e'_j$ が成り立つ. □

［補題 4.6］ R を可換環, M を R 加群とする. $M_1, M_2, \ldots, M_n$ および $N_1, N_2, \ldots, N_n$ を M の部分 R 加群とし,

$$M = \bigoplus_{i=1}^{n} M_i = \bigoplus_{i=1}^{n} N_i.$$

のように直和に分解されているものとする. さらに, すべての $i = 1, 2, \ldots, n$ に対して, $N_i \subseteq M_i$ であるとする. このとき, すべての $i = 1, 2, \ldots, n$ に対して, $N_i = M_i$ が成り立つ.

［証明］ 番号 j を任意にとり固定する. $x \in M_j$ とする. M が $N_1, N_2, \ldots, N_n$ の直和に分解されることから,

$$x = \sum_{i=1}^{n} x_i, \quad x_i \in N_i$$

と表せる. よって,

$$(x - x_j) + \sum_{i \neq j} x_i = 0_M.$$

すべての $i = 1, 2, \ldots, n$ に対して $N_i \subseteq M_i$ であるから,

$$\begin{aligned} &x - x_j \in M_j, \\ &x_i \in M_i \quad (i \neq j). \end{aligned}$$

M が $M_1, M_2, \ldots, M_n$ の直和に分解されることから, $x - x_j = 0_M$ を得る. よって,

$$x = x_j \in N_j.$$

ゆえに, $M_j \subseteq N_j$. したがって, $N_j = M_j$ となる. □

[補題 4.7] R を単項イデアル整域, $p_1, p_2, \ldots, p_t$ を R の素元とし, 2 つずつ互いに素であるとする. また,

$$M = \bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R \right)$$

とおく. このとき, 各 $i = 1, 2, \ldots, t$ に対して,

$$M(p_i) \cong \bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R.$$

また,

$$M = \bigoplus_{i=1}^{t} M(p_i).$$

さらに, p を R の素元とし, $p_1, p_2, \ldots, p_t$ と互いに素であるとすれば,

$$M(p) = \{0_M\}$$

となる.

[証明] 各 $i = 1, 2, \ldots, t$ に対して,

$$\iota_i : \bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R \to M$$

を入射とし, ι_i の像を N_i とおく:

$$N_i = \iota_i \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R \right).$$

すると, $N_i \subseteq M(p_i)$ であるから,

$$M = \sum_{i=1}^{t} M(p_i).$$

次に, $x_i \in M(p_i)$ $(i = 1, 2, \ldots, t)$ とし,

$$\sum_{i=1}^{t} x_i = 0_M$$

であるとする. 定理 2.1 より, $i = 1, 2, \ldots, t$ に対して, ある整数 $e_i \geq 0$ が存在して,

$$\mathrm{Ann}_R(x_i) = p_i^{e_i} R$$

が成り立つ. そこで, i を任意に 1 つ固定し,

$$q_i = \prod_{1 \leq j \leq t,\, j \neq i} p_j^{e_j}$$

とおくと,

$$x_i = -\sum_{1 \leq j \leq t,\, j \neq i} x_j,$$

$$q_i x_j = 0_M \quad (j \neq i)$$

であるから, $q_i x_i = 0_M$ である. R は単項イデアル整域であり, $p_i^{e_i}$ と q_i は互いに素であるから, ある $u, v \in R$ が存在して,

$$p_i^{e_i} u + q_i v = 1_R.$$

よって,

$$\begin{aligned} x_i &= 1_R \cdot x_i \\ &= u(p_i^{e_i} x_i) + v(q_i x_i) \\ &= 0_M. \end{aligned}$$

したがって, M は

$$M = \bigoplus_{i=1}^{t} M(p_i)$$

のように $M(p_1), M(p_2), \ldots, M(p_t)$ の直和に分解される. M は

$$M = \bigoplus_{i=1}^{t} N_i$$

のように $N_1, N_2, \ldots, N_t$ の直和に分解され, 各 $i = 1, 2, \ldots, t$ に対して $N_i \subseteq M(p_i)$ であるから, 補題 4.6 より, 各 $i = 1, 2, \ldots, t$ に対して $N_i = M(p_i)$ となる.

さて, p を R の素元とし, $p_1, p_2, \ldots, p_t$ と互いに素であるとする. $x \in M(p)$ とすると, ある整数 $e \geq 0$ が存在して,

$$p^e x = 0_M.$$

一方,

$$x = \sum_{i=1}^{t} x_i, \quad x_i \in N_i$$

と表すと,

$$0_M = p^e x = \sum_{i=1}^{t} p^e x_i.$$

各 $i = 1, 2, \ldots, t$ に対して, $p^e x_i \in N_i$ であるから,

$$p^e x_i = 0_M.$$

よって,

$$x_i \in M(p) \cap N_i.$$

$N_i = M(p_i)$ であるから,

$$x_i \in M(p) \cap M(p_i).$$

定理 2.3 より $M(p) \cap M(p_i) = \{0_M\}$ であるから, $x_i = 0_M$. ゆえに, $x = 0_M$. したがって, $M(p) = \{0_M\}$ となる. □

［補題 4.8］ R を単項イデアル整域, M を有限生成ねじれ R 加群, $p_1, p_2, \ldots, p_t$ を R の素元とし, M は

$$M = \bigoplus_{i=1}^{t} M(p_i)$$

のように直和に分解され, かつ

$$M(p_i) \neq \{0_M\} \quad (i = 1, 2, \ldots, t)$$

であるとする.

(i) $p_1, p_2, \ldots, p_t$ は 2 つずつ同伴でない.

(ii) $q_1, q_2, \ldots, q_{t'}$ を R の素元とし, $p_1, p_2, \ldots, p_t$ と同じ条件を満たしているとすれば,

$$\{p_i R \mid i = 1, 2, \ldots, t\} = \{q_i R \mid i = 1, 2, \ldots, t'\}$$

が成り立ち, $t = t'$ となる.

［証明］ (i) もし仮に p_1, p_2 が同伴であるとすれば, 定理 2.3 より $M(p_1) = M(p_2)$ であるから,

$$M(p_1) \cap M(p_2) = M(p_1) \neq \{0_M\}.$$

一方, M が $M(p_i)$ $(i = 1, 2, \ldots, n)$ の直和に分解されていることから,

$$M(p_1) \cap M(p_2) = \{0_M\}.$$

これは矛盾である. ゆえに, p_1, p_2 は同伴でない. 他の p_i, p_j $(i \neq j)$ についても同様である.

(ii)　もし仮に

$$q_1R \notin \{p_iR \mid i = 1, 2, \ldots, t\}$$

とすると, $M(q_1) \neq \{0_M\}$ より, ある整数 $e \geq 1$ と $x \in M$ が存在して,

$$q_1^e x = 0_M, \quad x \neq 0_M.$$

一方,

$$x = \sum_{i=1}^{t} x_i, \quad x_i \in M(p_i)$$

と表すと,

$$0_M = q_1^e x = \sum_{i=1}^{t} q_1^e x_i.$$

各 $i = 1, 2, \ldots, t$ に対して, $M(p_i)$ は M の部分 R 加群だから, $q_1^e x_i \in M(p_i)$. ゆえに,

$$q_1^e x_i = 0_M.$$

すなわち,

$$x_i \in M(p_1).$$

$x \neq 0_M$ より, ある番号 i_0 $(1 \leq i_0 \leq t)$ が存在して, $x_{i_0} \neq 0_M$. ゆえに,

$$M(q_1) \cap M(p_{i_0}) \neq \{0_M\}.$$

ところが, 仮定より q_1 と p_{i_0} とは同伴でないから, 定理 2.3 より

$$M(q_1) \cap M(p_{i_0}) = \{0_M\}.$$

これは矛盾である. よって,

$$q_1R \in \{p_iR \mid i = 1, 2, \ldots, t\}.$$

他の q_i についても同様である. ゆえに,

$$\{q_iR \mid i = 1, 2, \ldots, t'\} \subseteq \{p_iR \mid i = 1, 2, \ldots, t\}.$$

逆の包含関係も同じようにしていえるので, 等号が成り立つ. さらに, $p_1, p_2, \ldots, p_t$ は 2 つずつ同伴でないから, $p_1R, p_2R, \ldots, p_tR$ はすべて異なる. $q_1, q_2, \ldots, q_{t'}$ についても同様. したがって, $t = t'$ となる. □

［補題 4.9］ R を単項イデアル整域とする. $p_1, p_2, \ldots, p_t$ を R の素元とし, 2 つずつ互いに素であるとする. $q_1, q_2, \ldots, q_{t'}$ も同様とする. R 加群としての同型

$$\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R \right) \cong \bigoplus_{i=1}^{t'} \left(\bigoplus_{j=1}^{u'(i)} R/q_i^{f_{ij}} R \right) \tag{4}$$

が成り立ち, さらに i ごとに

$$\begin{aligned} &0 < e_{i,1} \le e_{i,2} \le \cdots \le e_{i,u(i)}, \\ &0 < f_{i,1} \le f_{i,2} \le \cdots \le f_{i,u'(i)} \end{aligned} \tag{5}$$

であるとする. このとき, $q_1, q_2, \ldots, q_{t'}$ の番号を適当に振りなおせば,

$$\begin{aligned} &t = t', \quad p_i R = q_i R \quad (i = 1, 2, \ldots, t), \\ &u(i) = u'(i) \quad (i = 1, 2, \ldots, t), \\ &e_{i,j} = f_{i,j} \quad (i = 1, 2, \ldots, t;\ j = 1, 2, \ldots, u(i)) \end{aligned}$$

となる.

［**証明**］式 (4) の右辺を M, 左辺を M' とおく. $f : M \to M'$ を R 同型とする. 補題 4.7 より,

$$M = \bigoplus_{i=1}^{t} M(p_i),$$
$$M' = \bigoplus_{i=1}^{t'} M'(q_i)$$

と表せる. ただし, $p_1, p_2, \ldots, p_t$ は互いに同伴でない R の素元である. $q_1, q_2, \ldots, q_{t'}$ も同様である. また, 定理 2.4 より, 各 $i = 1, 2, \ldots, t$ に対して

$$\begin{aligned} M(p_i) &\cong f\bigl(M(p_i)\bigr) \\ &= \bigl(f(M)\bigr)(p_i) \\ &= M'(p_i). \end{aligned} \tag{6}$$

よって,

$$\begin{aligned} M' &= f(M) \\ &= f\left(\bigoplus_{i=1}^{t} M(p_i)\right) \\ &= \bigoplus_{i=1}^{t} f\bigl(M(p_i)\bigr) \\ &= \bigoplus_{i=1}^{t} M'(p_i). \end{aligned}$$

ゆえに,

$$\bigoplus_{i=1}^{t} M'(p_i) = \bigoplus_{i=1}^{t'} M'(q_i).$$

補題 4.8 より,

$$\{p_i R \mid i = 1, 2, \ldots, t\} = \{q_i R \mid i = 1, 2, \ldots, t'\}$$

が成り立ち, $t = t'$ となる. $q_1, q_2, \ldots, q_{t'}$ の番号を適当に振りなおして, 各 $i = 1, 2, \ldots, t$ に対して, $p_i R = q_i R$ であるとしても一般性を失わない.

次に, 各 $i = 1, 2, \ldots, t$ に対して, 補題 4.7 より,

$$M(p_i) \cong \bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R,$$

$$M'(p_i) \cong \bigoplus_{j=1}^{u'(i)} R/p_i^{f_{ij}} R.$$

これと (6) より,

$$\bigoplus_{j=1}^{u(i)} R/p_i^{e_{ij}} R \cong \bigoplus_{j=1}^{u'(i)} R/p_i^{f_{ij}} R.$$

したがって, 補題 4.5 より, $u(i) = u'(i)$. またこのとき, $j = 1, 2, \ldots, u(i)$ に対して, $e_{ij} = f_{ij}$ が成り立つ. $\square$

参考文献

[1] 彌永昌吉, 有馬哲, 浅枝陽: 詳解代数入門, 東京図書, 1990.

[2] 松坂和夫: 代数系入門, 岩波書店, 1976.

[3] 森田康夫: 代数概論, 裳華房, 1987.