代数学 II 要約 NO.7

第 7 回目の主題：$\boxed{\text{PID 上の有限生成加群}}$

定義 7.1. 環 A 上の加群 M の元 $m_1, m_2, \dots, m_k$ に対して、 A-準同型

$$\varphi : A^{\oplus k} \ni \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} \mapsto \sum_{j=1}^{k} a_j . m_j$$

の核 $\mathrm{Ker}(\varphi)$ の元のことを $m_1, m_2, \dots, m_k$ の**関係式**と呼び、その全体のなす加群 $\mathrm{Ker}(\varphi)$ のことを $m_1, m_2, \dots, m_k$ の**関係式のなす加群**と呼ぶ。

以下では、次のような変換を考える。

(変換 1) $\{m_1, m_2, m_3, \dots, m_k\}$ の順序を入れ換える。

(変換 2) $\{m_1, m_2, m_3, \dots, m_k\}$ の代わりにそれを $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A)$ で「ひねった」

$$\{a.m_1 + b.m_2, c.m_1 + d.m_2, m_3, \dots, m_k\}$$

を考える。

(変換 3) $\{m_1, m_2, m_3, \dots, m_k\}$ の代わりに m_1 を

$$m_1' = m_1 + a_2 m_2 + a_3 m_3 + \dots m_k m_k$$

に置き換えたもの $\{m_1', m_2, m_3, \dots, m_k\}$ を考える。

(変換 3) は (変換 1), (変換 2) を有限回組み合わせて得られることがわかるので以下の議論で必須ではない。

補題 7.2. (変換 1),(変換 2),(変換 3) の形の変換は (同じ形の) 逆変換をもつ。とくに、$m_1, m_2, \dots, m_k$ が M を生成するならば、それに (変換 1),(変換 2),(変換 3) を有限回繰り返して得られた組み合わせ $m_1', m_2', \dots, m_k'$ も M を生成する。

補題 7.3. 可換 PID A と、その上の加群 M が与えられていて、M は A 上 $m_1, m_2, \dots, m_k$ で生成されているとする。$m_1, m_2, \dots, m_k$ を (変換 1), (変換 2), (変換 3) を有限回繰り返して得られる M の生成系の全体を $\mathcal{S}$ とおく。このとき、

(1) 各 $\underline{m'} = \{m_j'\} \in \mathcal{S}$ にたいして、

$$I_{\underline{m'}} = \{c_1 \in A; \sum_j c_j m_k \in M \qquad (\exists c_2, c_3, \dots c_k \in A)\}$$

とおくと、$I_{\underline{m'}}$ は A のイデアルである。

(2) $\{I_{\underline{m'}}; \quad m' \in \mathcal{S}\}$ のなかで (包含順序に関して) 極大なものが存在する。 その一つを以下 $J_{\underline{v}}$ と書こう。

(3) $J_{\underline{v}} = Ac$ となる c が存在する。 $c = 0$ なら M は自由加群である。以下、$c \neq 0$ とする。

(4)

$$a_1 v_1 + a_2 v_2 \dots + a_k v_k = 0 \qquad (a_1 = c)$$

なる関係式が存在する。

(5) 上の $a_1, a_2, a_3, \dots, a_k$ は c で割り切れる。(すなわち、Ac の元である。)

(6) $\underline{u} \in \mathcal{S}$ で、 $cu_1 = 0$ なるものが存在する。

(7) 上のような $\underline{u}$ の間に成り立つ任意の関係式

$$\sum_j c_j u_j = 0$$

にたいして、各 c_j は c で割り切れる。

(8) 上の $\underline{u}$ にたいして、M は Au_1 と $Au_2 + \dots + Au_k$ の直和と同型である。

上の補題のような M と $m_1, m_2, \dots m_k$ が与えられたとき、c に当たるものの候補を見付け、もしそれが「本物」ではない場合には証明にあるような操作を用いて生成元の変換を逐次行うことにより、u を求めるアルゴリズムを作成することができる。同様にして次の定理の w を得るアルゴリズムも得られる。

定理 7.4. 可換 PID A 上の有限生成加群 M が与えられているとする。このとき、M の生成系 $\underline{m} = \{m_1, m_2, \dots, m_k\}$ にたいして、$\underline{m}$ を (変換 1),(変換 2),(変換 3) を有限回繰り返すことにより、M の新しい生成系 $\underline{w}$ であって、

$$M \cong Aw_1 \oplus Aw_2 \oplus \dots Aw_k$$

となるものが存在する。

定義 7.5. 一つの元で生成される加群を**巡回加群**と呼ぶ。

補題 7.6. 任意の環 A に対して、次のことが言える。

(1) 任意の A の左イデアル J にたいして、 A/J は巡回加群である。
(2) 任意の巡回加群は (1) で述べたようなものと同型である。

命題 7.7. (定理の言い換え) 可換 PID A 上の任意の有限生成加群 M は巡回 A 加群の直和に同型である。ゆえに、ある $c_1, c_2, \dots, c_k \in A^k$ と

$$M \cong A/Ac_1 \oplus A/Ac_2 \oplus \dots \oplus A/Ac_k$$

なる同型が存在する。

(ただの) 加群は $\mathbb{Z}$-加群のことと同じであって、$\mathbb{Z}$ は PID であることから、つぎの (大変有用かつ重要な) 系が成り立つ。

系 7.8 (有限生成アーベル群の基本定理)**.** 任意の有限生成アーベル群は巡回群の有限個の直和である。

問題 7.1. $\mathbb{Z}$-加群 M が 2 つの元 m_1, m_2 で生成されていて、次の関係式を満たすとする。

$$30m_1 + 48m_2 = 0$$
$$88m_1 + 100m_2 = 0$$

これ以外に特段の関係式がないとするとき、m_1, m_2 に (変換 1),(変換 2),(変換 3) を有限回施すことにより、新しい生成元 w_1, w_2 を得て、M を巡回加群の直和として表現せよ。

復習:

命題 7.9. 可換 PID A の元 a, b に対して、イデアル $Aa + Ab$ はある単項イデアル Ad と等しい。このとき、ある a', b', x, y が存在して、次の二式が成り立つ。

(1) $a = a'd, \quad b = b'd.$
(2) $a'x + b'y = 1.$

とくに、

$$\begin{pmatrix} a' & b' \\ -y & x \end{pmatrix}$$

は $\mathrm{SL}_2(A)(\subset \mathrm{GL}_2(A))$ の元である。

命題 7.10. 可換 PID A のイデアルの増加列

$$I_1 \subset I_2 \subset I_3 \subset I_4 \subset \dots$$

は必ず有限で止まる。すなわち、ある N があって、

$$I_N = I_{N+1} = I_{N+2} = \dots$$

が成り立つ。