代数学３

水曜 2 限 (10:40∼12:10) **K202**
担当教員：加塩 朋和　　研究室：４号館３階
E-mail：kashio_tomokazu@ma.noda.tus.ac.jp

教科書・参考書

本講義は以下を参考にしました.

- 堀田良之著「代数入門 –群と加群–」裳華房
- 桂利行二著「代数学 II 環上の加群」東京大学出版会

なお, このレジュメは **LETUS** (`https://letus.ed.tus.ac.jp`) で配布しています. 順次, 加筆・修正したものをアップロードしていく予定です.

目 次

1　導入

1,2 年次の線型代数学において “体上の抽象ベクトル空間” を学んできた. 例えば $\mathbb{R}$ 上の抽象ベクトル空間とは (大まかに言って)

足し算と実数倍が “うまく” 定まっている空間

のことで, 例えば

- n 次元数ベクトル空間 $\mathbb{R}^n$.
- 実係数多項式全体のなす集合 $\mathbb{R}[X] = \{a_0+a_1X+\cdots+a_kX^k \mid a_0, \ldots, a_k \in \mathbb{R},\ k \geq 0\}$.
- n 次以下の実係数多項式全体のなす集合 $\mathbb{R}_{\leq n}[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_0, \ldots, a_n \in \mathbb{R}\}$.

などがある. ある. この “うまく” は, 演算の結合法則や分配法則を指している. 定義は非常に抽象的ながら, 結果として

任意の有限次元実ベクトル空間は $\mathbb{R}^n$ $(n \in \mathbb{N})$ と同型

になり, 体上の抽象ベクトル空間は, 思ったよりバリエーションがないことが分かる. (例えば $\mathbb{R}_{\leq n}[X] \cong \mathbb{R}^{n+1},\ a_0 + a_1X + \cdots + a_nX^n \mapsto \begin{bmatrix} a_0 \\ \vdots \\ a_n \end{bmatrix}$.)

この “体” を, より一般の “環” に取り替えたものが, <u>(環上の) 加群</u> と呼ばれる. 体上の抽象ベクトル空間に比べて, 環上の加群はバリエーション豊かである. 例えば $\mathbb{Z}$ 上の加群, すなわち, 足し算と整数倍が “うまく” 定まっている空間の例として

$$\mathbb{Z}^n, \quad \mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Q}$$

などがある.

この講義では環上の加群の理論の一般論を学ぶ. §2 ∼ 8 は基礎事項なのでしっかりやりたい. 集大成として

有限生成アーベル群に関する <u>アーベル群の基本定理</u> (§8, 系 36)

の紹介を目標とする.

一方で §9 (ジョルダン標準形), §10, 11 (射影加群, 入射加群), §12 (テンソル積), §13 (ネター加群, アルチン加群), §14 (群コホモロジーとピタゴラス数) は少し難しいので, 履修生の意見を聞いて, 重点的に扱う部分, スキップする部分を選択する.

2　環上の加群

定義 1. 空でない集合 R に, 以下を満たす二つの二項演算: 加法 $+$, 乗法 $\cdot$ が定義されているとき R は (これらの演算に関して) **環 (ring)** である, という.

(1) $(R, +)$ は加法群である. すなわち R は空でない集合で, 以下を満たす演算 $+$ が定義されている:

　(a) 結合法則: $\forall a, b, c \in R$, $(a + b) + c = a + (b + c)$.

　(b) 零元の存在: $\exists 0 = 0_R \in R$ s.t. $\forall a \in R$, $a + 0 = 0 + a = a$.
　(“どこの零元か” を強調する場合は 0_R のように表す.)

　(c) 加法逆元の存在: $\forall a \in R$, $\exists -a \in R$ s.t. $a + (-a) = (-a) + a = 0$.

　(d) 可換性: $\forall a, b \in R$, $a + b = b + a$.

(2) 乗法単位元の存在: $\exists 1 = 1_R \in R$ s.t. $\forall a \in R$, $a \cdot 1 = 1 \cdot a = a$.

(3) 乗法は次の結合法則を満たす: $\forall a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(4) 次の分配法則を満たす: $\forall a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

さらに

(5) $\forall a, b \in R$, $a \cdot b = b \cdot a$

をみたすとき, R は <u>可換環</u> である, という.

以下では

- R は (必ずしも可換とは限らない) 環とする. また乗法の記号 $\cdot$ は省略する ($ab := a \cdot b$).
- M を加法群 (すなわち $(M, +)$ が, 上の (a) $\sim$ (d) を満たす) とする.

定義 2. 加法群 M が <u>環 R 上の左加群</u>, または <u>左 R-加群 **(left R-module)**</u> であるとは, 作用と呼ばれる写像

$$R \times M \to M, \quad (r, m) \mapsto rm$$

が定まり, 以下を満たすことである.

(1) $\forall m \in M$, $1_R m = m$.

(2) $\forall r, s \in R$, $\forall m \in M$, $r(sm) = (rs)m$.

(3) $\forall r, s \in R$, $\forall m \in M$, $(r + s)m = (rm) + (sm)$.

(4) $\forall r \in R$, $\forall m, n \in M$, $r(m + n) = (rm) + (rn)$.

また (2) の代わりに

(2′) $\forall r, s \in R, \forall m \in M$, $r(sm) = (sr)m$.

を満たすとき, 右 R-加群 などと呼ぶ.

注意 3. (1) 右 R-加群 M の作用は rm ではなく mr と書くことが多い. この方が

(2′) $\forall r, s \in R, \forall m \in M$, $(ms)r = msr$.

と自然な表記になるからである.

(2) R が可換環のとき, 右加群と左加群は同じものとなり, 単に R-加群 などと呼ぶ. ただし, 非可換環の場合でも, 考えている作用が明らかな場合は, (左右を省略して) R-加群と書くことがある.

(3) 以下, 主に左加群の場合を考えるが, 右加群の場合も同様に議論できる.

例 4. (1) K が体のとき

$$V \text{ は } K\text{-ベクトル空間} \Leftrightarrow V \text{ は } K\text{-加群}.$$

(2) 環 R は, 通常の乗法に関して左 R-加群である. 右 R-加群でもある.

(3) 環 R の左 (右) イデアル I は, 通常の乗法に関して左 (右) R-加群である.

問題 1. $M_2(\mathbb{Z}) \times \mathbb{Z}^2 \to \mathbb{Z}^2$, $(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right], \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]) \mapsto \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \left[\begin{smallmatrix} ax+by \\ cx+dy \end{smallmatrix}\right]$ と置く. $\mathbb{Z}^2$ は左 $M_2(\mathbb{Z})$-加群であることを示せ.

問題 2. 左 R-加群 M に対して, 以下が成り立つことを示せ.

$$r0_M = 0_M,\ 0_R m = 0_M,\ (-r)m = -(rm) \qquad (r \in R,\ m \in M).$$

問題 3. 任意の加法群 M は

$$nm := \begin{cases} \underbrace{m + m + \cdots + m}_{n \text{ 個}} & (n > 0) \\ 0_M & (n = 0) \\ \underbrace{(-m) + (-m) + \cdots + (-m)}_{|n| \text{ 個}} & (n < 0) \end{cases} \quad (n \in \mathbb{Z},\ m \in M)$$

により $\mathbb{Z}$-加群となることを示せ.

定義 5. (1) M, N を左 R-加群とする. 写像 $f\colon M \to N$ が R 上の準同型, または R-準同型 (R-hom.) であるとは

$$f(rm) = rf(m),\ f(m + m') = f(m) + f(m') \quad (r \in R,\ m, m' \in M)$$

満たすことである. さらに f が全単射であれば, f は R-同型 (写像) であるといい, M, N は R-同型 (R-isom.) である, という. なお, 考えている環 R が明らかなとき, 単に準同型, 同型などと, R を省略することも多い. 以下も同様である.

(2) M を R 上の左加群とする．部分集合 $N \subset M$ が, 演算や作用の制限によって再び R 上の左加群になっているとき, N は M の **R 上の部分加群 (R-submodule)** である, という．すなわち (結果として以下を定義と思ってよい)

$$N \subset M \text{ が } R \text{ 上の部分加群} \Leftrightarrow \forall r \in R, \forall n, n' \in N,\ rn, -n, n+n' \in N.$$

(3) M を R 上の左加群, $N \subset M$ をその部分加群とする．このとき剰余群

$$M/N = \{m + N \mid m \in M\}$$

への R の作用

$$R \times (M/N) \to M/N,\ (r, m+N) \mapsto r(m+N) := rm + M$$

が定まり, M/N は R 上の左加群となり **剰余加群** と呼ばれる．

(4) M を R 上の左加群とし, $S \subset M$ を部分集合とする．M の任意の元が S の元の R 上の一次結合で表せるとき, S は M の **(R 上の) 生成系** である, という．すなわち

$$\begin{gathered} S \subset M \text{ が } R \text{ 上の生成系} \\ \overset{\text{def}}{\Leftrightarrow} \forall m \in M, \exists s_1, \ldots, s_k \in S, \exists r_1, \ldots, r_k \in R \text{ s.t. } m = r_1 s_1 + \cdots + r_k s_k. \end{gathered}$$

このとき

$$M = \langle s \mid s \in S \rangle_R, \quad M = \sum_{s \in S} Rs$$

などの表記をする．さらに S が有限集合 $s_1, \ldots, s_r$ であれば

$$M = \langle s_1, \ldots, s_r \rangle_R, \quad M = Rs_1 + \cdots + Rs_r$$

のようにも書く．M が有限個からなる生成系を持つとき, M は **有限生成 (fin. gen.)** である, などという．

例 6. (1) R の部分集合 I に対し

$$I \text{ は } R \text{ の左イデアル} \Leftrightarrow I \text{ は } (R \text{ 自身を左 } R\text{-加群と見たとき}) \ R \text{ の部分加群.}$$

よって, このとき左剰余集合 R/I も左 R-加群となる．

(2) M を R 上の左加群, $N_1, N_2 \subset M$ をその部分加群とする．このとき, これらの和と共通部分

$$N_1 + N_2 := \{n_1 + n_2 \mid n_1 \in N_1,\ n_2 \in N_2\},\ N_1 \cap N_2 := \{m \mid m \in N_1,\ m \in N_2\}$$

も M の部分加群となる．

(3) M, N を左 R-加群, $f\colon M \to N$ を R-準同型とする. このとき, 像と核

$$f(M) := \{f(m) \mid m \in M\} \subset N,\ \operatorname{Ker} f := \{m \in M \mid f(m) = 0_N\} \subset M$$

は, それぞれ N, M の部分加群となる.

(4) M, N を左 R-加群とする. このとき直和

$$M \oplus N := \{m \oplus n := (m, n) \mid m \in M,\ n \in N\}$$

も左 R-加群となる (集合としては直積集合. 元を $m \oplus n$ と表記する). また同じ左 R-加群 M の n 個の直和を M^n で表す.

(5) (有限個とは限らない) 左 R-加群 M_λ $(\lambda \in \Lambda)$ の直和は

$$\bigoplus_{\lambda \in \Lambda} M_\lambda := \{(m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda \in M_\lambda,\ m_\lambda \neq 0_{M_\lambda} \text{ となる } \lambda \in \Lambda \text{ は高々有限個 }\}$$

と定義する.

難問 4. 無限個の直和を $\{(m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda \in M_\lambda\}$ と定義しない理由を考えてみよ.

定理 7 (準同型定理)**.** M, N を左 R-加群, $f\colon M \to N$ を R-準同型とする. このとき,

$$\overline{f}\colon M/\operatorname{Ker} f \to f(M),\ m + \operatorname{Ker} f \mapsto f(m)$$

は R-同型写像となる.

証明. R-準同型は加法群としての群準同型写像でもあるので, 群の準同型定理 (例えば堀田良之著「代数入門 –群と加群–」裳華房, 定理 5.1, p24 参照) より $\overline{f}$ は加法群としての同型となる. 調べるべきは

$$\overline{f}(r(m + \operatorname{Ker} f)) \overset{?}{=} r\overline{f}(m + \operatorname{Ker} f)$$

である. 剰余加群の定義より $r(m+\operatorname{Ker} f) = rm+\operatorname{Ker} f$, f が R 準同型より $f(rm) = rf(m)$ であるので, 併せて

$$\overline{f}(r(m + \operatorname{Ker} f)) = \overline{f}(rm + \operatorname{Ker} f) \overset{*}{=} f(rm) = rf(m) \overset{*}{=} r\overline{f}(m + \operatorname{Ker} f)$$

を得る. なお $*$ は $\overline{f}$ の定義: $\overline{f}(m + \operatorname{Ker} f) = f(m)$ より従う. □

3　自由加群 (1)

定義 8. R を環とする.

(1) $a \in R$ が <u>**単元 (可逆元)**</u> $\overset{\text{def}}{\Leftrightarrow} \exists b \in R$ s.t. $ab = ba = 1$.

(2) 単元全体のなす集合を $R^\times$ で表し R の <u>**乗法群**</u> と呼ぶ. (掛け算に関して群となる.)

(3) $a \in R$ が <u>**零因子**</u> $\overset{\text{def}}{\Leftrightarrow} \exists b \in R, \neq 0$ s.t. $ab = 0$ or $ba = 0$.

(4) 零因子以外の元を <u>**正則元**</u> 呼ぶ.

定義 9. M を左 R-加群とする.

(1) $m \in M$ が <u>**ねじれ (torsion) 元**</u> $\overset{\text{def}}{\Leftrightarrow} \exists r \in R$: 正則元 s.t. $rm = 0_M$.

(2) M は <u>**ねじれ加群**</u> $\overset{\text{def}}{\Leftrightarrow} \forall m \in M$ がねじれ元.

(3) M は <u>**ねじれ無し (torsion-free) 加群**</u> である $\overset{\text{def}}{\Leftrightarrow} \forall m \in M, \neq 0_M$ がねじれ元でない.

問題 5. M を環 R 上の左加群とする. 以下を示せ.

(1) $\mathrm{Ann}_R\, m := \{r \in R \mid rm = 0_M\}$ $(m \in M)$, $\mathrm{Ann}_R\, M := \{r \in R \mid \forall m \in M,\ am = 0_M\}$ は, それぞれ R の左イデアルになる.

(2) 体 K 上の加群 (すなわち K-ベクトル空間) V は, ねじれ無し加群.

定義 10. M を環 R 上の左加群とする.

(1) $m_1, \ldots, m_n \in M$ が以下を満たすとき $m_1, \ldots, m_n$ は <u>**一次独立**</u> である, という.

$$r_1 m_1 + \cdots + r_n m_n = 0_M \ (r_1, \ldots, r_n \in R) \Rightarrow r_1 = \cdots = r_n = 0$$

また, $S \subset M$ が無限集合であるとき

$$S \text{ が一次独立} \overset{\text{def}}{\Leftrightarrow} \text{任意の有限部分集合} \subset S \text{ が一次独立.}$$

(2) $S \subset M$ が一次独立かつ生成系であるとき, S は M の <u>**(R 上の) 基底**</u> であるといい, 基底をもつ R 上の左加群 M を <u>**自由加群**</u> とよぶ.

注意 11. 便宜上, 零元のみからなる加群 $\{\mathbf{0}\}$ は, 空集合を基底とする自由加群とみなす.

定理 12. 体 K 上の加群 V には必ず基底が存在する. またその基底の濃度は一定である.

　この定理の証明の前にツォルンの補題を準備する. ツォルンの補題は選択公理と同値であり, この講義では成り立つと “仮定” している.

補題 13 (ツォルンの補題)**.** 空でない帰納的半順序集合は必ず極大元を持つ. ここで, 各言葉の定義は以下の通り:

(1) 集合 X 上の関係 $\preceq$ が <u>半順序</u> であるとは

(a) $\forall x \in X,\ x \preceq x.$

(b) $\forall x, y, z \in X,\ x \preceq y,\ y \preceq z \Rightarrow x \preceq z.$

(c) $\forall x, y \in X,\ x \preceq y,\ y \preceq x \Rightarrow x = y.$

を満たすことである. さらに

(d) $\forall x, y \in X,\ x \preceq y$ または $y \preceq x.$

を満たすものは <u>全順序</u> と呼ばれる. また, それぞれの場合, $(X, \preceq)$ を半順序集合, 全順序集合と呼ぶ.

(2) $(X, \preceq)$ を半順序集合とする. $x_0 \in X$ が <u>極大元</u>

$$\overset{\text{def}}{\Leftrightarrow} x_0 \preceq x \Rightarrow x = x_0.$$

(3) $(X, \preceq)$ を半順序集合とする. 部分集合 $Y \subset X$ が <u>上に有界</u>

$$\overset{\text{def}}{\Leftrightarrow} \exists x_0 \in X \text{ s.t. } \forall y \in Y,\ y \preceq x_0.$$

(4) 半順序集合 $(X, \preceq)$ が <u>帰納的</u> であるとは, 任意の空でない全順序部分集合 $Y \subset X$ が上に有界であることである.

定理 12 の証明. (基底の存在) ツォルンの補題を用いる. $V = \{\mathbf{0}\}$ なら空集合が基底. $V \neq \{\mathbf{0}\}$ とする. このとき

$$\mathcal{S} := \{ S \subset V \mid S \text{ は } K \text{ 上一次独立} \}$$

は通常の包含関係に関して空でない帰納的半順序集合となる. 実際

- $\boldsymbol{v} \in V, \neq \mathbf{0}$ は一次独立, すなわち $\{\boldsymbol{v}\} \in \mathcal{S}$. よって $\mathcal{S} \neq \emptyset$.
- $(\mathcal{S}, \subset)$ が半順序集合は明らかであろう.
- $Y \subset \mathcal{S}$ が空でない全順序部分集合とする. このとき $S_0 := \bigcup_{S \in Y} S$ は
  - $S_0 \in \mathcal{S}$.
    $\because$ $c_i \in K$, $\boldsymbol{v}_i \in S_0$, $\sum_{i=1}^n c_i \boldsymbol{v}_i = \mathbf{0}$ とする. $\boldsymbol{v}_i \in S_0 = \bigcup_{S \in Y} S$ より $\exists S_i \in Y$ s.t. $\boldsymbol{v}_i \in S_i$ $(i = 1, \ldots, n)$. Y は全順序集合なので, 有限部分集合 $\{S_i\}_{i=1,\ldots,n}$ には最大限 S_{i_0} が存在する. とくに $\forall i = 1, \ldots, n$, $\boldsymbol{v}_i \in S_i \subset S_{i_0}$. $S_{i_0} \in Y$ より $\{\boldsymbol{v}_i\}_{i=1,\ldots,n} \subset S_{i_0}$ は一次独立. よって $c_1 = \cdots = c_n = 0$ を得る.

– $\forall S \in Y,\ S \subset S_0$ ($\because\ S_0 = \bigcup_{S\in Y} S$).

を満たすので Y は上に有界である.

よってツォルンの補題より極大元 $B \in \mathcal{S}$ が取れる. $B \in \mathcal{S}$ より一次独立であり, さらに生成系でもあることが言えるので, B が V の基底を与える. 実際, $\boldsymbol{v}$ が B の要素達の一次結合で書けないとすると

$$B \subsetneq B \cup \{\boldsymbol{v}\} \in \mathcal{S}$$

より B が極大元であることに矛盾.

(有限基底の個数が一定) 線形代数の "基底の取り換え定理" から導くことができる (例えば吉野雄二著, 基礎課程–線形代数, サイエンス社, p96, 定理 7.4.2).

(無限基底の濃度が一定) もっと一般の場合 (補題 14) で成立する. □

補題 14. 可換環上 R の自由加群 M の一組の基底の濃度が無限集合であれば, M の基底の濃度は一定である.

証明. M に二組の基底 B, C が取れたとする. 各 $b \in B$ を基底 C の一次結合で表したとき, 現れる $c_i \in C$ 達からなる集合

$$b = \sum_{i=1}^{k_b} k_i c_i\ (k_i \in R, \neq 0) \Rightarrow C_b := \{c_1, \ldots, c_{k_b}\} \subset C$$

を考える. このとき

$$(\star) \qquad C = \bigcup_{b\in B} C_b$$

が言える. これを認めれば

$$|B|,\ |C|\ \text{のいずれかが有限集合ならともに有限集合}$$

($\because\ |B| < \infty \Rightarrow C = \bigcup_{b\in B}\{c_1, \ldots, c_{k_b}\}$ は有限個の有限集合の和集合だから $|C| < \infty$. B, C の役割を入れ替えて $|C| < \infty \Rightarrow |C| < \infty$) が言えて, B, C ともに無限集合としてよい. さらに

$$|C| \le \sum_{b\in B} |C_b| \le |B| \cdot |\mathbb{N}| = |B| \cdot \aleph_0 = |B|$$

より $|C| \le |B|$ を得て, B, C の役割を入れ替えて逆の不等号を得る. すなわち題意の $|B| = |C|$ が言えた. 以下 ($\star$) を示す. 一度も C_b に現れない $c_0 \in C$ が存在したとすると

- $C - \{c_0\}$ も M の生成系である.
  $\because$ M の任意の元は B の元の一次結合で書ける. B の各元 b は C_b の元の一次結合でかけるので, 代入すれば $\cup_{b\in B} C_b$ 達の一次結合でも書ける.

- とくに C は一次従属.
  $\because$ $c_0 \in M$ なのでこれも $C - \{c_0\}$ の元の一次結合 $c_0 = \sum_{c \in C, \neq c_0} k_c c$ で書ける. 移行して $c_0 - \sum_{c \in C, \neq c_0} k_c c = 0$ となるので一次従属.

よって矛盾. □

次の補題も証明にツォルンの補題を用いるので, ついでに紹介しておこう.

補題 15. 可換環 R のイデアル $I_0 \subsetneq R$ に対し I_0 を含む極大イデアルが存在する.

証明. $\mathcal{I} := \{I \subsetneq R \mid I$ は I_0 を含む R のイデアル $\}$ とおくと, 通常の包含関係に関して, 空でない帰納的半順序集合となる. 実際

- $I_0 \in \mathcal{I}$. よって $\mathcal{I} \neq \emptyset$.
- $(\mathcal{I}, \subset)$ が半順序の定義を満たすのは明らかであろう.
- $Y \subset \mathcal{I}$ が空でない全順序部分集合なら
$$\bigcup_{I \in Y} I \in \mathcal{I},\ \forall I \in Y,\ I \subset \bigcup_{I \in Y} I$$
  なので上に有界になる. ここで $\bigcup_{I \in Y} I \in \mathcal{I}$ のうち $\bigcup_{I \in Y} I \neq R$ のみ非自明であろう. これは $1 \notin \bigcup_{I \in Y} I$ と同値で, もし成り立たないとすると
$$1 \in \bigcup_{I \in Y} I \Rightarrow \exists I \in Y \subset \mathcal{I} \text{ s.t. } 1 \in I \Rightarrow I = R$$
  で $\mathcal{I}$ の定義に矛盾する.

よってツォルンの補題より, 極大元 $\exists M \in \mathcal{I}$. とくに M は I_0 を含む極大イデアル. □

注意 16. 体以外の環上の加群では, 必ずしも基底は取れない. 例えば $R = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$ に対し
$$R \times M \to M,\ (a, b \bmod n) \mapsto a(b \bmod n) := ab \bmod n$$
とおけば M は R 加群になる ($\because$ 例 6-(1)). このとき
$$\forall b \bmod n \in M,\ n(b \bmod n) = 0_M$$
であるから, M から一次独立な元はとることができない.

問題 6. 自由加群はねじれ無し加群であることを示せ.

問題 7. 問題 1 の左 $M_2(\mathbb{Z})$-加群 $\mathbb{Z}^2$ を考える. このとき

(1) $\mathbb{Z}^2$ は (左 $M_2(\mathbb{Z})$ 加群として) ねじれ無し加群である.

(2) $\mathbb{Z}^2$ は (左 $M_2(\mathbb{Z})$ 加群として) 自由加群でない.

ことを示せ.

略解. (1) $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \neq \mathbf{0}$ とすると $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \mathbf{0} \Rightarrow \det\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = 0 \Rightarrow \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ は零因子.

(2) 任意の $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbb{Z}^2$ が一次独立でない, すなわち “$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \mathbf{0} \Rightarrow \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \mathbf{0}$” が成り立たない. とくに基底が取れない. □

4　自由加群 (2)

定理 17. M を環 R 上の自由加群とし, その基底を B とおく. このとき R-同型

$$R^{\oplus B} \cong M,\ (a_b)_{b\in B} \mapsto \sum_{b\in B,\ a_b\neq 0} a_b b$$

が成り立つ. ここで $R^{\oplus B}$ は R の $|B|$ 個の直和

$$R^{\oplus B} := \bigoplus_{b\in B} R := \{(a_b)_{b\in B} \mid a_b \in R,\ a_b \neq 0 \text{ となる } b\in B \text{ は高々有限個}\}$$

とする. よって

$$M = \bigoplus_{b\in B} Rb,\ \sum_{b\in B} a_b b \mapsto (a_b b)_{b\in B}$$

により, 1 次元自由加群 $Rb := \{rb \in M \mid r \in R\}$ 達の直和と一致する (同一視できる).

証明. 写像 $R^{\oplus B} \to M$, $(a_b)_{b\in B} \mapsto \sum_{b\in B,\ a_b\neq 0} a_b b$ は明らかに R 準同型. さらにこの写像が

- 全射 $\Leftrightarrow \forall m \in M, \exists b_i \in B, \exists r_i \in R$ s.t. $m = r_1 b_1 + \cdots + r_k b_k \Leftrightarrow B$ が生成系.
- 単射 $\Leftrightarrow \mathrm{Ker} = \{0_{R^{\oplus B}}\} \Leftrightarrow [r_1 b_1 + \cdots + r_n b_n = 0_M\ (r_i \in R,\ b_i \in B) \Rightarrow r_1 = \cdots = r_n = 0] \Leftrightarrow B$ が一次独立. □

定理 18. 可換環 R 上の自由加群 M の基底の濃度は一定である. この濃度を自由加群 M の <u>階数</u> と呼び $\mathrm{rank}_R M$ で表す.

問題 8. R を環とする. 左 R-加群 M と両側イデアル $I \subset R$ を考える. 以下を確かめよ.

(1) $IM := \{\sum_{k=1}^{l} i_k m_k \mid l \geq 0,\ i_k \in I,\ m_k \in M\}$ は M の部分加群になる.

(2) 剰余加群 M/IM は, 作用

$$\overline{r}\,\overline{m} := \overline{rm}$$

により R/I-加群になる. ここで以下の自然な射影を考えている.

$$R \to R/I,\ r \mapsto \overline{r} := r + I,$$
$$M \to M/IM,\ m \mapsto \overline{m} := m + IM.$$

(3) $S \subset M$ が R 上の生成系であれば $\overline{S} := \{\overline{s} \mid s \in S\} \subset M/IM$ は R/I 上の生成系.

定理 *18* 証明. 無限濃度の基底が存在するときは補題 14 で示した. よって二組の有限個からなる基底 $b_1, \ldots, b_m$, $c_1, \ldots, c_n$ が取れたと仮定して

$$M = \bigoplus_{i=1}^{m} Rb_m = \bigoplus_{i=1}^{n} Rc_n \Rightarrow m = n$$

を言えばよい. まず定理 15 より極大イデアル $\mathfrak{m} \subset R$ が取れる. $K := R/\mathfrak{m}$ は体だから

($\star$) $b_1, \ldots, b_m$ が M の R 上の基底であれば $\overline{b_1}, \ldots, \overline{b_m}$ は $M/\mathfrak{m}$ の K 上の基底になる

ことを言えば良い. すると $\overline{b_1}, \ldots, \overline{b_m}, \overline{c_1}, \ldots, \overline{c_n}$ はともに体 K 上の加群 $M/\mathfrak{m}M$ の基底となるので, 定理 12 より $m = n$ を得る. さらに上の問題より

($\star\star$) $b_1, \ldots, b_m$ が R 上一次独立であれば $\overline{b_1}, \ldots, \overline{b_m}$ は $M/\mathfrak{m}$ は K 上一次独立になる

を言えば ($\star$) が言える. 実際

$$\begin{aligned}
&\sum_{i=1}^{m} \overline{r_i}\overline{b_i} = 0_{M/\mathfrak{m}M} \ (r_i \in R) \\
&\Rightarrow \sum_{i=1}^{m} r_i b_i \in \mathfrak{m}M.
\end{aligned}$$

ここで $\mathfrak{m}M$ の一般元は M の元の $\mathfrak{m}$ 係数一次結合であり, さらに M の一般元は $b_1, \ldots, b_m$ の一次結合なので, $\mathfrak{m}M$ の一般元は $b_1, \ldots, b_m$ の $\mathfrak{m}$ 係数一次結合でかける. すなわち

$$\Rightarrow \sum_{i=1}^{m} r_i b_i = \sum_{j=1}^{m} m_j b_j \ (\exists m_j \in \mathfrak{m}).$$

さらに $b_1, \ldots, b_m$ は一次独立なので

$$\begin{aligned}
&\Rightarrow \forall i, r_i = m_i \in \mathfrak{m} \\
&\Rightarrow \forall i, \ \overline{r_i} = 0_K.
\end{aligned}$$

□

命題 19. R を可換環とし, 有限階数自由 R-加群 M とその基底 $b_1, \ldots, b_n$ を考える. このとき $c_1, \ldots, c_n \in M$ 対し以下は同値.

(1) $c_1, \ldots, c_n$ は M の基底.

(2) $\exists A \in GL_n(R) := \{A \in M_n(R) \mid \det A \in R^\times\}$ s.t. $\begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} = \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} A.$

また, このような正則行列 A を 基底の変換行列 などと呼ぶ.

まず以下の補助的な命題を示す.

命題 20. R を可換環とする. 全行列環 $M_n(R)$ の乗法群は

$$GL_n(R) := M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$$

で与えられる. なお $GL_n(R)$ は 一般線形群 と呼ばれる.

証明. 線形代数での証明と同様に示せる (係数が体 K なら $\det A \in K^\times \Leftrightarrow \det A \neq 0$ に注意). 示すべきは $A \in M_n(R)$ に対し

$$\exists B \in M_n(R) \text{ s.t. } AB = BA = E_n \Leftrightarrow \det A \in R^\times.$$

($\Rightarrow$) $\det A \det B = \det(AB) = \det E_n = 1$ より. ($\Leftarrow$) 余因子行列の転置 ${}^t\tilde{A}$ が ${}^t\tilde{A}A = A\,{}^t\tilde{A} = (\det A)E_n$ を満たすので $\det A \in R^\times$ なら $B := \det A^{-1}\,{}^t\tilde{A}$ が題意を満たす. □

命題 *19* 証明. $b_1,\dots,b_n$ は生成系なので, 各元 $c_j \in M$ は

$$c_j = \sum_{i=1}^{n} a_{ij} b_j \quad (a_{ij} \in R)$$

の形にかける. これを集めて

$$\begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} = \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} A \quad (A := [a_{ij}] \in M_n(R))$$

という表記を得る.

<u>(1) ⇒ (2)</u> $c_1,\dots,c_n$ も生成系だから, 役割を入れ替えて

$$\begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} B \quad (B \in M_n(R))$$

という表記も得られる. 先の式に (または先の式を) 代入して

$$\begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix} BA, \ \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} = \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} AB.$$

ここで $c_1,\dots,c_n$ は一次独立なので, 各 c_j を $c_1,\dots,c_n$ の一次結合で表す方法は

$$c_j = 0c_1 + \cdots + 0c_{j-1} + 1c_j + 0c_{j+1} + \cdots + 0c_n$$

のみ. すなわち BA の第 j 列は基本ベクトル $\boldsymbol{e}_j$ となる. よって $BA = \begin{bmatrix} \boldsymbol{e}_1 & \cdots & \boldsymbol{e}_n \end{bmatrix} = E_n$. 同様に $AB = E_n$ も得る.

<u>(1) ⇐ (2)</u> $c_1,\dots,c_n$ が生成系であること：任意の元 $m \in M$ は, 生成系 $b_1,\dots,b_n$ の一次結合 $m = \sum_{i=1}^{n} r_i b_i$ $(r_i \in R)$ で書ける. よって

$$m = \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} A^{-1} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

となる. $A \in GL_n(R)$ より $A^{-1} \in M_n(R)$, とくに $A^{-1} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \in R^n$ だから m は $c_1,\dots,c_n$ の一次結合で表せている.

$c_1,\dots,c_n$ が一次独立であること： $\sum_{i=1}^{n} r_i c_i = 0$ $(r_i \in R)$ とする. このとき

$$0 = \sum_{i=1}^{n} r_i c_i = \begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} A \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

と書け, $b_1,\dots,b_n$ は一次独立なので $A \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \mathbf{0}$ を得る. 両辺に A^{-1} をかけて $r_1 = \cdots = r_n = 0$ を得た. □

5　自由加群 (3)

この節の結果は, 線形代数で習った方法でも証明可能であるが, ここでは <u>可換図式</u> を使って説明してみる.

命題 21. R を可換環とし, 有限階数自由 R-加群 M, N と, それぞれの基底 $b_1, \ldots, b_m$, $c_1, \ldots, c_n$ を考える. R-準同型写像 $f\colon M \to N$ に対し

$$\begin{bmatrix} f(b_1) & \cdots & f(b_m) \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_n \end{bmatrix} A_f$$

を満たす行列 $A_f \in M_{n\times m}(R)$ がただ一つ定まり, 基底 $b_1, \ldots, b_m$, $c_1, \ldots, c_n$ に関する f の <u>表現行列</u> などと呼ばれる. この表現行列は, 定理 17 での同型により

$$i\colon R^m \cong M,\ i(\begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}) := [b_1\ \cdots\ b_m] \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix},$$
$$j\colon R^n \cong N,\ j(\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}) := [c_1\ \cdots\ c_n] \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

と同一視した場合, A_f は f を表す行列となっている. すなわち

$A_f \in M_{n\times m}(R)$ が f の表現行列

$$\Leftrightarrow \text{図式}\ \begin{tikzcd} M \arrow[r, "f"] & N \\ R^m \arrow[u, "i", "\wr"'] \arrow[r, "\boldsymbol{v} \mapsto A_f \boldsymbol{v}"'] & R^n \arrow[u, "j", "\wr"'] \end{tikzcd}\ \text{が可換}\ \left(\overset{\text{i.e.}}{\Leftrightarrow} \forall \boldsymbol{v} \in R^m,\ j(A_f \boldsymbol{v}) = (f \circ i)(\boldsymbol{v}) \right).$$

証明. (前半) 性質を満たす A_f が取れるのは $b_1, \ldots, b_m$ が生成系より. 一意性は $b_1, \ldots, b_m$ が一次独立より. (後半) 可換図式の成立

$$\Leftrightarrow \forall \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix},\ f([b_1\ \cdots\ b_m] \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}) = [c_1\ \cdots\ c_n] A_f \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}$$
$$\overset{f\ \text{は}\ R\text{-準同型}}{\Leftrightarrow} \forall \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix},\ [f(b_1)\ \cdots\ f(b_m)] \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix} = [c_1\ \cdots\ c_n] A_f \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}. \cdots (*)$$

一方で, A_f が f の表現行列 $\Leftrightarrow [f(b_1)\ \cdots\ f(b_m)] = [c_1\ \cdots\ c_n] A_f \cdots (**)$.
$(*) \Leftarrow (**)$ は明らか. $(*) \Rightarrow (**)$ は, $\begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}$ として単位ベクトルを持ってくれば分かる. □

問題 9. 上の証明中では以下を使っている. それぞれ証明せよ.

(1) R-準同型写像の合成写像は R-準同型写像.

(2) R-同型写像の逆写像は R-同型写像 (特に R-準同型写像).

(3) $f\colon R^m \to R^n$ が R-準同型写像であれば, 以下を満たす行列 $A = A_f \in M_{n\times m}(R)$ が唯一つ存在する: $\forall \boldsymbol{v} \in R^m,\ f(\boldsymbol{v}) = A\boldsymbol{v}$.

定理 22. R を可換環とし, 有限階数自由 R-加群 L, M, N, それぞれの基底 $a_1, \ldots, a_l$, $b_1, \ldots, b_m$, $c_1, \ldots, c_n$, 及び R-準同型写像 $f\colon L \to M$, $g\colon M \to N$ を考える. 基底 a_*, b_* に関する f の表現行列を A, 基底 b_*, c_* に関する g の表現行列を B とおくとき, 基底 a_*, c_* に関する $g \circ f\colon L \to N$ の表現行列は BA になる.

証明. 可換図式

$$\begin{tikzcd} L \arrow[r, "f"] & M \arrow[r, "g"] & N \\ R^l \arrow[u, "\boldsymbol{u} \mapsto [a_1 \, \cdots \, a_n]\boldsymbol{u}"] \arrow[r, "\boldsymbol{u} \mapsto A\boldsymbol{u}"'] & R^m \arrow[u, "\boldsymbol{v} \mapsto [b_1 \, \cdots \, b_m]\boldsymbol{v}"] \arrow[r, "\boldsymbol{v} \mapsto B\boldsymbol{v}"'] & R^n \arrow[u, "\boldsymbol{w} \mapsto [c_1 \, \cdots \, cT_l]\boldsymbol{w}"] \end{tikzcd}$$

を考える. 上段を一番左から一番右までいくと $g \circ f$ である. 一方で, 下段を一番左から一番右までいくと $\boldsymbol{v} \mapsto BA\boldsymbol{v}$ である. よって, 上での可換図式の議論により題意を得る. □

問題 10. R を可換環とし, 有限階数自由 R-加群 M と, 二組の基底 $b_1, \ldots, b_m$, $b'_1, \ldots, b'_m$ を考える. 基底 $\boldsymbol{b}_*$ から基底 $\boldsymbol{b}'_*$ への変換行列を P とおく. このとき R-準同型写像 $\mathrm{id}_M\colon M \to M$ の基底 $\boldsymbol{b}_*$, $\boldsymbol{b}'_*$ に関する表現行列が P^{-1} になることを確かめよ.

定理 23. R を可換環とし, 有限階数自由 R-加群 M, N と, それぞれ二組の基底 $b_1, \ldots, b_m$, $b'_1, \ldots, b'_m$, $c_1, \ldots, c_n$, $c'_1, \ldots, c'_n$ を考える. 基底 b_* から基底 b'_* への変換行列を P, 基底 c_* から基底 c'_* への変換行列を Q とおく. このとき R-準同型写像 $f\colon M \to N$ の基底 b_*, c_* に関する表現行列が A であれば, 同じ R-準同型写像 f の基底 b'_*, c'_* に関する表現行列は $Q^{-1}AP$ となる.

証明. 仮定より可換図式

$$\begin{tikzcd} M & M \arrow[l, "\mathrm{id}_M"'] \arrow[r, "f"] & N \arrow[r, "\mathrm{id}_N"] & N \\ R^m \arrow[u, "\boldsymbol{u} \mapsto [b'_1 \, \cdots \, b'_m]\boldsymbol{u}"] & R^m \arrow[l, "{P^{-1}\boldsymbol{u} \leftarrow\!\shortmid \boldsymbol{u}}"', "{\boldsymbol{u} \mapsto P\boldsymbol{u}}"'] \arrow[u, "\boldsymbol{u} \mapsto [b_1 \, \cdots \, b_m]\boldsymbol{u}"] \arrow[r, "\boldsymbol{u} \mapsto A\boldsymbol{u}"'] & R^n \arrow[u, "\boldsymbol{v} \mapsto [c_1 \, \cdots \, c_n]\boldsymbol{v}"] \arrow[r, "\boldsymbol{v} \mapsto Q^{-1}\boldsymbol{v}"'] & R^n \arrow[u, "\boldsymbol{v} \mapsto [c'_1 \, \cdots \, c'_n]\boldsymbol{v}"] \end{tikzcd}$$

を得る. 上段を一番左から一番右までいくと $\mathrm{id}_N \circ f \circ \mathrm{id}_M^{-1} = f$, 下段を一番左から一番右までいくと $\boldsymbol{u} \mapsto Q^{-1}AP\boldsymbol{u}$ なので題意を得る. □

6　単因子論 (1)

R を可換環とし, 有限階数自由 R-加群 M と R-準同型写像 $f\colon M \to M$ を考える. 定理 23 より, 適当な基底に関する表現行列 A_f は基底の取り換えにより

$$QA_fP \quad (Q \in GL_n(R),\ P \in GL_m(R))$$

の形に書き換えることができる. “うまい基底の取り方” により QA_fP をできるだけ簡単な表記にすることは, 応用上重要である. また命題 21 より, この “うまい基底の取り方” は “うまく $P \in GL_m(R), Q \in GL_n(R)$ を選ぶ” ことと同値である. ここでは, 特に R が **PID (単項イデアル整域)** の場合に限り議論する. すなわち

- R は可換環.
- $a, b \in R$, $a, b \neq 0 \Rightarrow ab \neq 0$.
- $I \subset R$: イデアル $\Rightarrow \exists d \in R$ s.t. $I = (d) := Rd = \{rd \mid r \in R\}$.

を仮定する. 例えば

- 任意の体. この場合任意のイデアルは (0) である.
- 有理整数環 $\mathbb{Z}$.
- 体 K 係数の一変数多項式環 $K[T]$.

は PID である.

問題 11. 体係数二変数多項式環 $K[S,T]$ や整数係数多項式環 $\mathbb{Z}[T]$ は PID でない. この理由を説明せよ.

定義 24. (1) 単位行列の (i,i), (i,j), (j,i), (j,j)-成分を, それぞれ $\alpha, \beta, \gamma, \delta$ に置き換えた行列 $(i \neq j)$

$$E_{ij}(\alpha,\beta,\gamma,\delta) := \begin{array}{cc} & \begin{array}{ccccccccccc} &&& \text{第 } i \text{ 列} &&&& \text{第 } j \text{ 列} &&& \end{array} \\ \begin{array}{c} \\ \\ \\ \text{第 } i \text{ 行} \\ \\ \\ \\ \text{第 } j \text{ 行} \\ \\ \\ \\ \end{array} & \begin{bmatrix} 1 &&&&&&&&&& \\ & \ddots &&&&&&&&& \\ && 1 &&&&&&&& \\ &&& \alpha &&&& \beta &&& \\ &&&& 1 &&&&&& \\ &&&&& \ddots &&&&& \\ &&&&&& 1 &&&& \\ &&& \gamma &&&& \delta &&& \\ &&&&&&&& 1 && \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& 1 \end{bmatrix} \end{array}$$

のうち

$$\det E_{ij}(\alpha,\beta,\gamma,\delta)=\det\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}=\alpha\delta-\beta\gamma\in R^\times$$

となるものを <u>基本行列</u> と呼ぶ.

(2) $A\in M_{n\times m}(R)$ に, 左からサイズ n の基本行列, または右からサイズ m の基本行列をかけることを, 行列の <u>基本変形</u> と呼ぶ.

(3) 行列に有限回基本変形を行うことを <u>初等変形</u> と呼ぶ.

問題 12. 以下を確かめよ.

(1) $A\in M_{n\times m}(R)$ を初等変形で $B\in M_{n\times m}(R)$ に変形できるとき $A\sim B$ と表すとき, $\sim$ は $M_{n\times m}(R)$ 上の同値関係である.

(2) $E_{ij}(\alpha,0,0,1)$ $(\alpha\in R^\times)$ を左からかける $\Leftrightarrow$ 第 i 行を α 倍.

(3) $E_{ij}(0,1,1,0)$ を左からかける $\Leftrightarrow$ 第 i,j 行を入れ替え.

(4) $E_{ij}(1,\beta,0,1)$ $(\beta\in R)$ を左からかける $\Leftrightarrow$ 第 j 行を β 倍して第 i 行に加える.

なお (2), (3), (4) は “右, 行” を “左, 列” に取り換えても成り立つ.

定理 25. R を PID とする. このとき, 任意の行列 $A\in M_{n\times m}(R)$ は初等変形により

$$\begin{bmatrix}d_1 &&&&&\\ & d_2 &&&&\\ && \ddots &&&\\ &&& d_r &&\\ &&&& 0 &\\ &&&&& \ddots\end{bmatrix},\ d_1|d_2|\cdots|d_r,\ d_r\neq 0$$

の形にできる. ただし $d,d'\in R$ に対し

$$d|d'\Leftrightarrow \exists r\in R \text{ s.t. } d'=dr$$

と定める. また, 行列 A に対し $d_1,d_2,\ldots,d_r$ は単元倍 (すなわち $R^\times$ の元倍) を除いて一意的に定まり A の <u>単因子</u> と呼ばれる.

<u>単因子の一意性以外</u> の証明. A に初等変形を施して得られる行列全体のなす集合を

$$\mathcal{A}:=\{B\in M_{n\times m}(R)\mid A\sim B\}$$

とおき, さらに各 $B\in\mathcal{B}$ の成分で生成される単項イデアル全体のなす集合を

$$\mathcal{I}:=\{(a)\mid \exists B=[b_{ij}]\in\mathcal{A},\ \exists i,j \text{ s.t. } a=b_{ij}\}$$

とおく. このとき

Claim1. $\mathcal{I}$ には極大元が存在する．すなわち $\exists(d) \in \mathcal{I}$ s.t. $(d) \subset (a) \in \mathcal{I} \Rightarrow (d) = (a)$.

$\because$ もし極大元が存在しなければ

- 適当に $(a_1) \in \mathcal{I}$ をとる

$\Rightarrow$ (a_1) は極大元でないので $(a_1) \subsetneq \exists(a_2) \in \mathcal{I}$.

$\Rightarrow$ (a_2) も極大元でないので $(a_2) \subsetneq \exists(a_3) \in \mathcal{I}$.

$\Rightarrow$ 同様に繰り返して $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$ $((a_n) \in \mathcal{I})$ とできる．

$\Rightarrow$ $I := \cup_{n\in\mathbb{N}}(a_i)$ は R のイデアルになることが示せる．PID より $\exists a \in I$ s.t. $I = (a)$.
つまり $a \in (a) = \cup_{n\in\mathbb{N}}(a_i)$. 和集合の定義より $\exists m \in \mathbb{N}$ s.t. $a \in (a_m)$.

$\Rightarrow$ よって $(a_m) \subset \cup_{n\in\mathbb{N}}(a_i) = (a) \subset (a_m)$ となりこれらは一致する．

$\Rightarrow$ よって $(a_m) = \cup_{n\in\mathbb{N}}(a_i) \supset (a_{m+1}) \supsetneq (a_m)$. これは矛盾．

さて, 一つ極大元 $(d) \in \mathcal{I}$ を固定する．定義より $\exists B \sim A$ s.t. B のある成分が d. さらに行, 列の入れ替えは基本変形であったので, B の $(1,1)$-成分が d としてよい．このとき

Claim2. B の $(1,j)$-成分, $(j,1)$-成分はすべて (d) の元．

$\because$ B の $(1,j)$-成分を b とし, $I := (d,b) = \{xd + yb \mid x, y \in R\}$ とおく．このとき PID より $\exists a \in I$ s.t. $I = (a)$. さらに

- $d, b \in I = (a)$ より $\exists d_0, a_0 \in R$ s.t. $d = d_0 a$, $b = b_0 a$.
- $a \in (a) = I = (d,b)$ より $\exists x, y \in R$ s.t. $a = xd + yb$.

これらを合わせて $a = xd + yb = xd_0 a + yb_0 a$, i.e., $a(1 - xd_0 - yb_0) = 0 \overset{\text{整域}}{\Rightarrow} xd_0 + yb_0 = 1$, i.e., $E_{1j}(x, y, d_0, -b_0)$ は基本行列, が分かる．この基本行列 $E_{1j}(x, y, d_0, -b_0)$ を左から B にかけると, $(1,1)$-成分が $xd + yb = a$ になる．とくに $(a) \in \mathcal{I}$. よって

$$(d) \subset (d,b) = (a)$$

だから, (d) の極大性より $(d) = (a)$. よって $b \in (d,b) = (a) = (d)$ が従う．$(j,1)$-成分の場合も同様に示せる．

この Claim2 より B の $(1,j)$-成分, $(j,1)$-成分は $d\alpha$ $(\alpha \in R)$ の形なので基本行列 $E_{1j}(1, -\alpha, 0, 1)$ をかけることで 0 にできる．すなわち

$$A \sim B = \begin{bmatrix} d & d* & \dots & d* \\ d* & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ d* & * & \dots & * \end{bmatrix} \sim \begin{bmatrix} d & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{bmatrix}$$

と基本変形できる．サイズが一つ小さい $\begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix}$ の部分に同様の操作を行うことを繰り返して

$$\sim \begin{bmatrix} d_1 := d & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{bmatrix}$$

とできる．さて

$$E_{12}(1,1,0,1) \begin{bmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{bmatrix} = \begin{bmatrix} d_1 & d_2 & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{bmatrix}$$

だから $\begin{bmatrix} d_1 & d_2 & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{bmatrix} \in \mathcal{A}$．よって Claim2 より $d_1|d_2$．同様に $d_1|d_2|\cdots|d_r$ が言える． $\square$

7　単因子論 (2)

単因子の一意性 を証明するために少し準備を行う.

定義 26. R を PID とする. $A=[a_{ij}]\in M_{n\times m}(R)$ に対して, r 行 r 列を抜き出してサイズ r の行列を作り, その行列式をとったものを A の r 次小行列式 と呼ぶ. また, この r 次小行列式全体の最大公約元 $\Delta_r(A)$ を A の 行列式因子 と呼ぶ $(1\le r\le \min\{m,n\})$. すなわち

$$(\Delta_r(A)):=\left(\det\begin{bmatrix}a_{k_1l_1} & a_{k_1l_2} & \cdots & a_{k_1l_r}\\ a_{k_2l_1} & a_{k_2l_2} & \cdots & a_{k_2l_r}\\ \vdots & \vdots & \ddots & \vdots\\ a_{k_rl_1} & a_{k_rl_2} & \cdots & a_{k_rl_r}\end{bmatrix} \mid \begin{array}{c}1\le k_1<k_2<\cdots<k_r\le n\\ 1\le l_1<l_2<\cdots<l_r\le m\end{array}\right).$$

ただし $(*)$ は $*$ で生成される R のイデアルを表す.

定理 27. 行列式因子は初等変形で (単元倍を除いて) 不変である.

証明. $A\sim B$ のとき $\Delta_r(A)|\Delta_r(B)$ を言えばよい (A,B を入れ替えて $\Delta_r(B)|\Delta_r(A)$ が言え, $d|d'$ かつ $d'|d$ から $\exists u\in R^\times$ s.t. $d'=ud$ が言える). 初等変形は基本変形の繰り返しであるから, 基本行列 $E_{ij}(\alpha,\beta,\gamma,\delta)$ $(\alpha\delta-\beta\gamma\in R^\times)$ により

$$B=E_{ij}(\alpha,\beta,\gamma,\delta)A \text{ または } AE_{ij}(\alpha,\beta,\gamma,\delta)$$

と書けたとしてもよい. 後者も同様なので, 以下は前者 $B=E_{ij}(\alpha,\beta,\gamma,\delta)A$ を仮定して議論する. 基本行列 $E_{ij}(\alpha,\beta,\gamma,\delta)$ を左からかけると, 第 i, j 行のみ変化することに注意して, 小行列式 $\det\begin{bmatrix}a_{k_1l_1} & a_{k_1l_2} & \cdots & a_{k_1l_r}\\ a_{k_2l_1} & a_{k_2l_2} & \cdots & a_{k_2l_r}\\ \vdots & \vdots & \ddots & \vdots\\ a_{k_rl_1} & a_{k_rl_2} & \cdots & a_{k_rl_r}\end{bmatrix}$ がどう変化するか考えると, 以下が分かる.

(1) $i,j\notin\{k_1,\dots,k_r\}$ のとき $\cdots$ 変化なし.

(2) $i\in, j\notin\{k_1,\dots,k_r\}$ のとき $\cdots$ $\det\begin{bmatrix}a_{k_1l_1} & \cdots & a_{k_1l_r}\\ \vdots & & \vdots\\ a_{il_1} & \cdots & a_{il_r}\\ \vdots & & \vdots\\ a_{k_rl_1} & \cdots & a_{k_rl_r}\end{bmatrix} \rightsquigarrow \det\begin{bmatrix}a_{k_1l_1} & \cdots & a_{k_1l_r}\\ \vdots & & \vdots\\ \alpha a_{il_1}+\beta a_{jl_1} & \cdots & a_{il_r}+\beta a_{jl_r}\\ \vdots & & \vdots\\ a_{k_rl_1} & \cdots & a_{k_rl_r}\end{bmatrix}$

$$=\alpha\det\begin{bmatrix}a_{k_1l_1} & \cdots & a_{k_1l_r}\\ \vdots & \vdots & \vdots\\ a_{il_1} & \cdots & a_{il_r}\\ \vdots & \vdots & \vdots\\ a_{k_rl_1} & \cdots & a_{k_rl_r}\end{bmatrix}+\beta\det\begin{bmatrix}a_{k_1l_1} & \cdots & a_{k_1l_r}\\ \vdots & \vdots & \vdots\\ a_{jl_1} & \cdots & a_{jl_r}\\ \vdots & \vdots & \vdots\\ a_{k_rl_1} & \cdots & a_{k_rl_r}\end{bmatrix}\in(\Delta_r(A)).$$

(3) $i\notin, j\in\{k_1,\dots,k_r\}$ のとき $\cdots$ 上と同様.

(4) $i, j \in \{k_1, \dots, k_r\}$ のとき $\cdots$ $\det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix} \rightsquigarrow \det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ \alpha a_{il_1}+\beta a_{jl_1} & \cdots & \alpha a_{il_r}+\beta a_{jl_r} \\ \vdots & \vdots & \vdots \\ \gamma a_{il_1}+\delta a_{jl_1} & \cdots & \gamma a_{il_r}+\delta a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix}$

$$= \alpha\gamma \det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix} + \alpha\delta \det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix} + \beta\gamma \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix} + \beta\delta \det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix}$$

$$= (\alpha\delta - \beta\gamma) \det \begin{bmatrix} a_{k_1l_1} & \cdots & a_{k_1l_r} \\ \vdots & \vdots & \vdots \\ a_{il_1} & \cdots & a_{il_r} \\ \vdots & \vdots & \vdots \\ a_{jl_1} & \cdots & a_{jl_r} \\ \vdots & \vdots & \vdots \\ a_{k_rl_1} & \cdots & a_{k_rl_r} \end{bmatrix} \in (\Delta_r(A)).$$

ここで, 途中の式変形は行列式の多重線形性を用いた. 結局, $B = E_{ij}(\alpha, \beta, \gamma, \delta)A$ のすべての r 次小行列式が $(\Delta_r(A))$ に含まれるので $(\Delta(B)) \subset (\Delta_r(A))$, すなわち $\Delta_r(A)|\Delta_r(B)$ が従う. □

系 28. R を PID とする. 行列 $A \in M_{n\times m}(R)$ を (定理 25 で示した通り) 初等変形により

$$\begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \end{bmatrix}, \ d_1|d_2|\cdots|d_r, \ d_r \neq 0$$

と変形できたとする. このとき

$$\Delta_1(A) = d_1, \ \Delta_2(A) = d_1d_2, \dots, \ \Delta_r(A) = d_1d_2\cdots d_r.$$

とくに行列 A の単因子 $d_1, \dots, d_r$ は一意的に定まる.

証明. 上の定理より $\Delta_1(A) = \Delta_1(\begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \end{bmatrix})$. 行列式因子の定義より

$$(\Delta_1(\begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \end{bmatrix})) = (d_1, d_2, \dots, d_r, 0, \dots, 0) \overset{\because\ d_1|d_2|\cdots|d_r}{=} (d_1).$$

よって (単元倍を除いて) $\Delta_1(A) = d_1$. 同様に $\Delta_k(A) = \Delta_k(\begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \end{bmatrix}) = d_1 d_2 \cdots d_k$ が言える. またこのとき (R が整域なのでその商体を考えて) $d_k = \Delta_k(A)\Delta_{k-1}(A)^{-1}$ となり, 一意性が従う. □

以下の結果は次節で用いる.

定義 29. R を可換環とする. 以下の同値な定義を満たすとき, R を (可換) ネター環 と呼ぶ.

(1) R の任意のイデアルは有限生成.

(2) R のイデアルからなる空でない集合は包含関係に関して極大元を持つ.

(3) R のイデアルからなる増大列 $I_1 \subset I_2 \cdots$ はどこかで止まる. すなわち, ある n が存在して $I_n = I_{n+1} = \cdots$ となる.

補題 30. ネター環 R 上の有限生成加群 M の部分加群 N は有限生成である.

証明. M が n 元生成 であるとし, n に関する帰納法を用いる. $n = 1$ のとき

$$M = Rm$$

である. 全射 R-準同型写像

$$f \colon R \to M,\ r \mapsto rm$$

を考えると $f^{-1}(N)$ は R の部分加群であり, 従って R のイデアルとなる. R はネター環だったので $I = (r_1, \ldots, r_k) = \sum_{j=1}^k Rr_j$ と書ける. よって

$$N = f(I) = \sum_{j=1}^{k} R(r_j m)$$

という表記を得る.

次に $1 \sim n-1$ で成立すると仮定し, n のときを考える. $M = \sum_{i=1}^n Rm_i$ とかける. 自然な射影

$$\pi \colon M \to \overline{M} := M/Rm_n$$

を考える. このとき剰余加群 $\overline{M}$ は

$$\overline{M} = \sum_{i=1}^{n-1} R\pi(m_i)$$

と書けるので $n-1$ 元生成である. よって帰納法の仮定より, 部分加群 $N \subset M$ に対し

$$\pi(N) \subset \overline{M}$$

は有限生成となり, 生成系 $\pi(n_1), \ldots, \pi(n_k)$ が取れる. 一方で 1 元生成加群 Rm_n の部分加群

$$N \cap Rm_n \subset Rm_n$$

を考えると, やはり仮定より有限生成となり, 生成系 $n'_1, \ldots, n'_l$ が取れる. このとき $n_1, \ldots, n_k, n'_1, \ldots, n'_l$ が N の生成系を与える. 実際, 任意の $n \in N$ に対し $\exists r_i$ s.t.

$$\pi(n) = \sum_{i=1}^{k} r_i \pi(n_i).$$

よって

$$n - \sum_{i=1}^{k} r_i n_i \in N \cap (\operatorname{Ker} \pi) = N \cap Rm_n$$

となり, これは $n'_1, \ldots, n'_l$ の一次結合として書ける. $\square$

注意 31. PID ならネター環でもある ($\because$ 定義の (1) を満たす). 特に

PID 上の有限生成加群の部分加群は有限生成

である.

8 単因子論 (3)

定理 32. R を PID とし, M を R 上の有限生成加群とする. このとき M は

$$R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k \oplus R^l \quad (d_i \in R, \notin R^\times, \neq 0,\ d_1 \mid d_2 \mid \cdots \mid d_k,\ 0 \leq k, l \in \mathbb{Z})$$

の形の加群と R-同型となる. また, このような d_i, k, l は M に対して (d_i は単元倍を除いて) 一意的に定まる. ここで

$$a \mid b \quad \overset{\text{def}}{\Leftrightarrow} \quad \text{“}a \text{ は } b \text{ を割り切る”} \quad \overset{\text{def}}{\Leftrightarrow} \quad b \in Ra.$$

また, 同型により

$$M = R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k \oplus R^l$$

を同一視することで, $R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k$, R^l は M の部分加群とみなせる. このとき

- $R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k :=$ “M の <u>ねじれ部分</u>”.
- $R^l :=$ “M の <u>自由部分</u>”.

と呼ぶ. $(d_1, \ldots, d_k), l$ を M の <u>単因子型</u> などと呼ぶ.

証明. 先に一意性以外を示す. M の生成系を $x_1, \ldots, x_m$ とおく. このとき, 写像

$$g\colon R^m \to M,\ (a_1, \ldots, a_m) \to a_1x_1 + \cdots + a_mx_m$$

は R 上の全射準同型となる. またその核 $\operatorname{Ker} g$ は, 注意 32 より再び有限生成になるので, 同様に R 上の全射準同型

$$f_0\colon R^n \to \operatorname{Ker} g$$

が構成できる. f_0 と自然な単射 $\operatorname{Ker} g \hookrightarrow R^m$ を合成して

$$f\colon R^n \to R^m$$

を考える. このとき f_0 が全射, すなわち $f(R^n) = f_0(R^n) = \operatorname{Ker} g$ に注意. よって準同型定理より

$$M \cong R^m/\operatorname{Ker} g = R^m/f(R^n)$$

を得る. ここで $f\colon R^n \to R^m$ を適当な基底による表現表列 $F \in M_{m\times n}(R)$ をとる. F は初等変形によって

$$\begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix},\ d_1|d_2|\cdots|d_r,\ d_r \neq 0$$

の形にできる．すなわち $\exists$ 正則行列 Q, P s.t. $Q^{-1}FP = \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix}$．この P, Q で R^n, R^m の基底を取り換えることで

$$\exists y_1, \dots, y_n\text{: } R^n \text{ の基底}, \exists z_1, \dots, z_m\text{: } R^m \text{ の基底 s.t. } f(y_i) = \begin{cases} d_i z_i & (1 \le i \le k), \\ 0 & (i > k) \end{cases}$$

と書ける．よって

$$\begin{aligned} M \cong R^m/f(R^n) &= \left(\bigoplus_{i=1}^m Rz_i\right) \Big/ f\left(\bigoplus_{i=1}^n Ry_i\right) \\ &= \left(\bigoplus_{i=1}^m Rz_i\right) \Big/ \left(\bigoplus_{i=1}^k Rd_i z_i\right) \cong \left(\bigoplus_{i=1}^k R/Rd_i\right) \oplus R^{m-k} \end{aligned}$$

を得る．

続いて一意性を証明する．M のねじれ元全体

$$TM := \{x \in M \mid \exists a \in R, \neq 0 \text{ s.t. } ax = 0\}$$

は M のねじれ部分と一致し, M の部分加群となる．また剰余加群

$$\begin{aligned} T/TM &\cong (R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k \oplus R^l)/(R/Rd_1 \oplus R/Rd_2 \cdots \oplus R/Rd_k) \\ &\cong R^l \end{aligned}$$

は階数 l の自由加群となる．よって, 定理 18 より, l は M により一意的に定まる．ねじれ部分の一意性は少々複雑であるので, 証明の概略を箇条書きにするにとどめる．

(a) PID は UFD (素元分解整域, 一意分解整域) でもある．とくに, 各 d_i の素元分解

$$d_i = u_i p_1^{n_{i1}} p_2^{n_{i2}} \cdots p_r^{n_{ir}} \quad (u_i \in R^\times,\ p_j \text{ は互いに同伴でない素元},\ n_{ij} \ge 0)$$

を考えることができる．また $d_1 \mid d_2 \mid \cdots \mid d_k$ より

$$n_{1j} \le n_{2j} \le \cdots \le n_{kj}.$$

(b) 中国剰余定理より

$$R/Rd_i \cong \bigoplus_{j=1}^r R/Rp_j^{n_{ij}}, \quad \text{よって} \quad TM \cong \bigoplus_{i=1}^k \bigoplus_{j=1}^r R/Rp_j^{n_{ij}}.$$

(c) 素元 p_j を一つ固定して M の p_j ねじれ元全体

$$M(p_j) := \{x \in M \mid \exists n \in \mathbb{N} \text{ s.t. } p_j^n x = 0\}$$

を考える．これは M の部分加群であり

$$M(p_j) \cong \bigoplus_{i=1}^k R/Rp_j^{n_{ij}}.$$

(d) 下の補題 を $M(p_j)$ に使うと, 各素元 p_j に関し (c) の $\{n_{1j}, \dots, n_{kj}\}$ は M により一意的に定まることが分かる. よって $d_i = u_i p_1^{n_{i1}} p_2^{n_{i2}} \cdots p_r^{n_{ir}}$ も, 単元倍を除いて一意的に定まる. □

注意 33. (a) PID ⇒ UFD に関して, 例えば堀田良之著「代数入門 –群と加群–」裳華房, 定理 9.2, p47 参照.

注意 34. (b) 中国剰余定理に関して, 例えば堀田良之著「代数入門 –群と加群–」裳華房, 系 9.1, p50 参照.

問題 13. R を PID, $p \in R$ を素元とし, R-加群 $M := R/Rp^n$ を考える.

(1) M の任意の元は p ねじれ元である (i.e., $R/Rp^n(p) = R/Rp^n$) こと示せ.

(2) $p^kM/p^{k+1}M \cong \begin{cases} R/Rp & (k < n) \\ \{0\} & (k \geq n) \end{cases}$ を示せ.

(3) $q \in R$ を p と同伴でない素元とする. このとき M の q ねじれ部分は自明な元のみであること (i.e., $R/Rp^n(q) = \{0\}$) を示せ.

(4) 上の証明中の (c) を示せ.

略解. (1) $\overline{x} \in R/Rp^n \Rightarrow p^n\overline{x} = \overline{p^nx} = 0 \in R/Rp^n$.

(2) (1) の証明中で $p^nM = \{0\}$ が言えているので後半が従う. 前半は

$$f\colon R \to p^kM/p^{k+1}M,\ x \mapsto p^k\overline{x} + p^{k+1}M$$

は明らかに全射 R-準同型なので, 核が Rp になることを言えば, 準同型定理より従う. 実際 $x \in \operatorname{Ker} f \Leftrightarrow p^k\overline{x} \in p^{k+1}M \Leftrightarrow \exists y \in R$ s.t. $p^kx \equiv p^{k+1}y \bmod p^n \overset{k<n}{\Leftrightarrow} \exists y \in R$ s.t. $x \equiv py \bmod p^{n-k} \Leftrightarrow x \in Rp + Rp^{n-k} = Rp$.

(3) $\overline{x} \in R/Rq^n$, $p^k\overline{x} = 0\ (k \in \mathbb{N}) \overset{?}{\Rightarrow} \overline{x} = 0$ を言えばよい. 例えば素元分解 $x = ul_1^{n_1} \cdots l_r^{n_r}$ を考えれば $p^k\overline{x} = 0 \Rightarrow q^n \mid ul_1^{n_1} \cdots l_r^{n_r}p^k \overset{p,q\text{ は同伴でない}}{\Rightarrow} \exists i$ s.t. l_i と q は同伴で $n_i \geq n \Rightarrow q^n \mid ul_1^{n_1} \cdots l_r^{n_r} = x \Rightarrow \overline{x} = 0$.

(4) (1), (3) より. □

補題 35. R を PID とし, その素元 p と 有限生成 R-加群 M を考える. さらに M の任意の元は p ねじれ元, すなわち

$$\forall x \in M,\ \exists n \in \mathbb{N} \text{ s.t. } p^nx = 0$$

を満たすと仮定する. このとき

$$M \cong R/Rp^{n_1} \oplus \cdots \oplus R/Rp^{n_u}$$

満たす単調増加列 $n_1 \leq \cdots \leq n_u$ がただ一つ存在する.

証明. p ねじれ元はねじれ元でもあるから $M = TM$. よって上での議論により $M = TM \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r} R/Rp_j^{n_{ij}}$ と書ける. さらに上の問題の (3) より p 以外の素元は現れないことが分かる. すなわち

$$M \cong R/Rp^{n_1} \oplus \cdots \oplus R/Rp^{n_u} \quad (n_1 \leq \cdots \leq n_u)$$

の形に書けることが分かった. 以下この表記が一意的であることを示す. 上の問題の (2) より

$$p^k M/p^{k+1}M \cong (R/Rp)^{N_k}, \quad N_k := \text{“}n_1, \ldots, n_u \text{ のうち}, k \text{ 未満のものの個数”}$$

となる. この N_k は

$$N_k = \operatorname{rank}_{R/Rp} p^k M/p^{k+1}M$$

とも書けるので M により定まる. よって数列 $n_1 \leq \cdots \leq n_u$ も唯一つに定まる. □

系 36 (アーベル群の基本定理)**.** 有限生成アーベル群は有限個の巡回群の直積と同型である. より詳しく, 以下が成り立つ: G を有限生成アーベル群とする. このとき, 群同型

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^l \quad (d_1 \mid \cdots \mid d_r,\ d_i \in \mathbb{N},\ 0 \leq r, l \in \mathbb{Z})$$

を満たす $d_1, \ldots, d_r, l$ がただ一組存在する.

9　ジョルダン標準形

定理 32 で与えた単因子型 $(d_1, \ldots, d_k), l$ も, 各 d_i の素元分解も一意的であることから, 定理 32 の証明中の (b) で与えた表記も一意的であることが分かる.

系 37. R を PID とし, M を R 上の有限生成加群とする. このとき M のねじれ部分 TM は

$$TM \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{k_j} R/Rp_j^{n_{ij}} \quad (p_j \text{ は互いに同伴でない素元},\ 1 \leq n_{1j} \leq \cdots \leq n_{k_j j})$$

の形に表せる. また $\{(p_j, \{n_{ij}\}_{i=1,\ldots,k_j})\}_{j=1,\ldots,r}$ は M により (単元倍を除いて) 唯一つに定まり, ねじれ部分の <u>素因子型</u> などと呼ばれる.

この節の目的は, 線形代数学で学んだ以下の定理の, 単因子論による再証明である.

定理 38. K を代数的閉体とする. $r \in \mathbb{N}$, $\alpha \in K$ に対し

$$J_r(\alpha) := \begin{bmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \alpha & 1 \\ & & & & \alpha \end{bmatrix} \in M_r(K)$$

を (サイズ r の) <u>ジョルダンブロック</u> (ジョルダンセル, ジョルダン細胞などとも) と呼ぶ.

V を K 上の n 次元ベクトル空間とし, $f\colon V \to V$ を K 上の線形写像とする. このとき, V の基底をうまく選んで, f の行列表示を, いくつかのジョルダンブロックを並べた行列

$$\begin{bmatrix} J_{r_1}(\alpha_1) & & & \\ & J_{r_2}(\alpha_2) & & \\ & & \ddots & \\ & & & J_{r_m}(\alpha_m) \end{bmatrix} \quad (m \in \mathbb{N},\ r_1 + \cdots + r_m = n,\ \alpha_1, \ldots, \alpha_m \in K)$$

にできる. このような表現行列を f の <u>ジョルダン標準形</u> と呼ぶ. また, 線形写像 f を表すジョルダン標準形は, ジョルダンブロックの並び替えを除いて一意的である.

注意 39. 体 K が代数的閉体であるとは

任意の K 係数多項式 $K[X]$ が $K[X]$ の中で一次式の積に表せる

ことである. 例えば $K = \mathbb{C}$ は代数的閉体である (代数学の基本定理).

以下証明を与える. V を K 上の n 次元ベクトル空間とし, $f\colon V \to V$ を K 上の線形写像とする. $R := K[T]$ (一変数多項式環) とし, R の V への作用を

$$R \times V \to V,\ (p(T), x) \mapsto p(f)x$$

で定めると, V は R-加群となる. ただし $p(T) = c_0 + c_1 T + \cdots + c_k T^k$ $(c_i \in K)$ に対し

$$p(f)x := c_0 x + c_1 f(x) + \cdots + c_k f^k(x),\ f^i := \underbrace{f \circ f \circ \cdots \circ f}_{i\text{ 個}}$$

と定める.

問題 14. V は R-加群となることを示せ.

さらに V は K 上 n 次元より, R 上も有限生成であることが分かる. ($\because$ V の K 上の基底 $v_1, \ldots, v_n$ は, $V = \langle v_1, \ldots, v_n \rangle_K \overset{K \subset R}{\subset} \langle v_1, \ldots, v_n \rangle_R$ より, V の R 上の生成系にもなる.) よって $R = K[T]$ は PID なので, 上の系より

$$V \cong \left(\bigoplus_{j=1}^{r} \bigoplus_{i=1}^{k_j} R/Rp_j^{n_{ij}} \right) \oplus R^l,$$
$$p_j \in R \text{ は互いに同伴でない素元},\ 1 \le n_{1j} \le \cdots \le n_{k_j j},\ l \ge 0$$

となる. ここで

- もし $l \neq 0$ なら $\dim_K R = \infty$ より V が有限次元に矛盾.
- 代数的閉体 K 上の一変数多項式環 $K[T]$ の素元は一次式 $T - \alpha$ $(\alpha \in K)$ の形.

であるから, 結局

$$\Phi\colon V \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{k_j} R/R(T-\alpha_j)^{n_{ij}},\ \alpha_j \in K \text{ は相異なる},\ 1 \le n_{1j} \le \cdots \le n_{k_j j}$$

と書ける. このとき右辺の各 $R/R(T-\alpha_j)^{n_{ij}}$ に対応する V の部分空間 V_{ij} に適当な基底を与えることで, $f|_{V_{ij}}$ の表現行列がジョルダンブロックになる. 実際

- R-加群としての同型 $V \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{k_j} R/R(T-\alpha_j)^{n_{ij}}$ において, 左辺の $f\colon V \to V$ は, 右辺の T 倍写像 と対応する.
- 右辺において $R/R(T-\alpha_j)^{n_{ij}}$ は T 倍写像で安定であるため, 対応する部分空間 $V_{ij} := \Phi^{-1}(R/R(T-\alpha_j)^{n_{ij}})$ は f 安定部分空間となる.

- K-ベクトル空間 $R/R(T-\alpha)^r$ の基底として $e_a := (T-\alpha)^{r-a}$ $(a = 1, \ldots, r)$ が取れる. この基底に関する T 倍写像の表現行列は $J_r(\alpha)$ となる. 実際

$$\begin{aligned} f(e_1, \ldots, e_r) &= [T(T-\alpha)^{r-1}, \ldots, T(T-\alpha)^1] \\ &= [(T-\alpha)^r + \alpha(T-\alpha)^{r-1}, \ldots, (T-\alpha)^2 + \alpha(T-\alpha)] \\ &= [0 + \alpha e_1, \ldots, e_{r-2} + \alpha e_{r-1}] \quad (\because (T-\alpha)^r = 0 \in R/R(T-\alpha)^r) \\ &= [e_1 \ \cdots \ e_r] \begin{bmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \alpha & 1 \\ & & & & \alpha \end{bmatrix}. \end{aligned}$$

- V_{ij} の基底として $\Phi^{-1}((T-\alpha_j)^{n_{ij}-a})$ $(a = 1, \ldots, n_{ij}-1)$ をとれば, $f|_{V_{ij}}$ の表現行列は $J_{n_{ij}}(\alpha_j)$ となる. またこれらを集めて V の基底とすれば, 表現行列はジョルダン標準形の形になる.

後はジョルダン標準形が一意的であることを言えばよい. これは f の行列表示が

$$\begin{bmatrix} J_{r_1}(\alpha_1) & & & \\ & J_{r_2}(\alpha_2) & & \\ & & \ddots & \\ & & & J_{r_m}(\alpha_m) \end{bmatrix} \quad (m \in \mathbb{N},\ r_1 + \cdots + r_m = n,\ \alpha_1, \ldots, \alpha_m \in K)$$

とかけることは, R-加群としての同型

$$V \cong \bigoplus_{j=1}^{m} R/R(T-\alpha_j)^{r_j}$$

があることを意味し (下の問題), 素因子型の一意性から (α_j, r_j) 達の一意性が従う.

問題 15. 各ジョルダンブロック $J_{r_j}(\alpha_j)$ に対応する基底 $v_{j1}, \ldots, v_{jr_j}$ で張られる V の部分空間を V_j とおく. このとき以下を示せ.

(1) V_j は f 安定部分空間. よって R-加群としても部分加群となる.

(2) R-部分加群 V_j において, T 倍写像は $f|_{V_j}$ と一致する. とくに

$$T(v_{j1}, \ldots, v_{jr_j}) = [v_{j1} \ \cdots \ v_{jr_j}] J_{r_j}(\alpha_j) = [\alpha_j v_{j1} \ \cdots \ v_{j(r_j-1)} + \alpha_j v_{jr_j}].$$

(3) 以下は R-加群としての同型を与える.

$$V_j \cong R/R(T-\alpha_j)^{r_j},\ v_{ji} \mapsto (T-\alpha_j)^{r_j-i}.$$

10 射影加群, 入射加群 (1)

定義 40. L, M, N などは加法群, f, g などは (群としての) 準同型写像とする. また $M \xrightarrow{f} N$ で M から N への準同型写像を表す.

(1) $L \xrightarrow{f} M \xrightarrow{g} N$ が <u>完全列</u> (または <u>完全</u>) $\overset{\text{def}}{\Leftrightarrow} \operatorname{Im} f = \operatorname{Ker} g$.

(2) $\cdots \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \to \cdots$ が<u>完全列</u> (または <u>完全</u>)
$\overset{\text{def}}{\Leftrightarrow}$ 各 $M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2}$ が完全列
$\Leftrightarrow \forall i, \operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$.

(3) <u>短完全列</u> とは, 完全列

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

のことである. ただし

(a) 零元のみからなる加群 $\{0\}$ を 0 と略記する.

(b) 準同型写像 $0 \to L$ は $0 \mapsto 0$ しか存在しないので明記しない.

(c) 準同型写像 $N \to 0$ は $n \mapsto 0$ しか存在しないので明記しない.

問題 16. 以下を示せ.

(1) $0 \to N \xrightarrow{f} M$ が完全 $\Leftrightarrow$ f が単射.

(2) $M \xrightarrow{f} N \to 0$ が完全 $\Leftrightarrow$ f が全射.

(3) 部分加群 $N \subset M$ に対して剰余加群 M/N を考えたとき

$$0 \to N \xrightarrow{\text{自然な単射 } i} M \xrightarrow{\text{自然な射影}\pi} M/N \to 0$$

は短完全列となる.

略解. (1) 準同型 $N \to 0, n \mapsto 0$ の像は $\{0\}$. よって完全 $\Leftrightarrow \{0\} = \operatorname{Ker} f \Leftrightarrow f$ が単射.
(2) 準同型 $N \to 0$ の核は N. よって完全 $\Leftrightarrow \operatorname{Im} f = N \Leftrightarrow f$ が全射.
(3) (1), (2) より $N \xrightarrow{i} M \xrightarrow{\pi} M/N$ の部分のみ確かめればよい. □

注意 41. 左 R-加群としての準同型写像は加法群としての準同型写像でもあったので, 完全列の定義は左 R-加群, R-準同型写像に関しても定義されていることに注意. 右 R-加群でも同様.

以下では R を環とし, L, M, N などは左 R-加群, f, g などは R-準同型写像とする.

命題 42. (1) $\mathrm{Hom}_R(M,N) := \{f\colon M \to N \mid f$ は R-準同型写像$\}$ とおく. このとき

$$(f+g)(m) := f(m) + g(m)$$

により $\mathrm{Hom}_R(M,N)$ は加法群となる.

(2) $\phi\colon N \to L$ により誘導される写像を

$$\phi_*\colon \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,L),\ f \mapsto \phi \circ f$$

で定める. これは (加法群としての) 準同型写像となる.

(3) $\phi\colon L \to M$ により誘導される写像を

$$\phi^*\colon \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(L,N),\ f \mapsto f \circ \phi$$

で定める. これは (加法群としての) 準同型写像となる.

証明. 明らか. □

問題 17. 以下を確かめよ.

(1) $\mathrm{Hom}_R(R,M) \to M,\ f \mapsto f(1)$ は加法群として同型.

(2) $\mathrm{Hom}_R(L,N) \oplus \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(L \oplus M, N),\ f \oplus g \mapsto [l \oplus m \mapsto f(l) + g(m)]$ は加法群として同型.

(3) $\mathrm{Hom}_R(L,N) \oplus \mathrm{Hom}_R(L,M) \to \mathrm{Hom}_R(L, N \oplus M),\ f \oplus g \mapsto [l \mapsto f(l) \oplus g(l)]$ は加法群として同型.

略解. 群準同型写像であることは明らか. 以下が逆写像を与えているので全単射.
(1) $M \to \mathrm{Hom}_R(R,M),\ m \mapsto [r \mapsto rm]$.
(2) $\mathrm{Hom}_R(L \oplus M, N) \to \mathrm{Hom}_R(L,N) \oplus \mathrm{Hom}_R(M,N),\ f \mapsto [l \mapsto f(l \oplus 0_M)] \oplus [m \mapsto f(0_L \oplus m)]$.
(3) $\pi_1\colon N \oplus M \to N, n \oplus m \mapsto n$, $\pi_2\colon N \oplus M \to M, n \oplus m \mapsto m$ とおき, $\mathrm{Hom}_R(L, N \oplus M) \to \mathrm{Hom}_R(L,N) \oplus \mathrm{Hom}_R(L,M),\ f \mapsto \pi_1 \circ f \oplus \pi_2 \oplus f$. □

命題 43. (1) 完全列 $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ と, 任意の N に対し

$$0 \to \mathrm{Hom}_R(N,M_1) \xrightarrow{f_*} \mathrm{Hom}_R(N,M_2) \xrightarrow{g_*} \mathrm{Hom}_R(N,M_3)$$

も完全列.

(2) 完全列 $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ と, 任意の N に対し

$$0 \to \mathrm{Hom}_R(M_3,N) \xrightarrow{g^*} \mathrm{Hom}_R(M_2,N) \xrightarrow{f^*} \mathrm{Hom}_R(M_1,N)$$

も完全列.

証明. (1) f が単射 $\Leftrightarrow \operatorname{Ker} f = \{0\} \Leftrightarrow [f(m) = 0 \Leftrightarrow m = 0]$ に注意. よって

$$\begin{aligned}
&\phi \in \operatorname{Ker} f_* = \{\phi \in \operatorname{Hom}_R(N, M_1) \mid f \circ \phi = 0\} \\
&\Rightarrow \forall n \in N,\ f(\phi(n)) = 0 \Rightarrow \forall n \in N,\ \phi(n) = 0 \Rightarrow \phi = 0,
\end{aligned}$$

すなわち f_* は単射となる.

次に $\operatorname{Im} f \subset \operatorname{Ker} g \Leftrightarrow g \circ f = 0$ に注意. よって

$$g_* \circ f_* = [\phi \mapsto g \circ f \circ \phi = 0 \circ \phi] = 0,$$

すなわち $\operatorname{Im} f_* \subset \operatorname{Ker} g_*$ となる.

最後に $\operatorname{Im} f_* \supset \operatorname{Ker} g_*$ を示す.

$$\begin{aligned}
\phi \in \operatorname{Ker} g_* &\Leftrightarrow \phi \in \operatorname{Hom}_R(N, M_2),\ g \circ \phi = 0 \\
&\Rightarrow \operatorname{Im} \phi \subset \operatorname{Ker} g \subset \operatorname{Im} f,
\end{aligned}$$

すなわち, ϕ の値域の制限により

$$\phi_0 \colon N \to \operatorname{Im} f$$

とみなせる. また f は単射より, やはり値域を制限して

$$f_0 \colon M_1 \cong \operatorname{Im} f$$

となる ($\because$ 準同型定理). よって

$$\psi := [f_0^{-1} \circ \phi_0 \colon N \to M_1] \in \operatorname{Hom}_R(N, M_1)$$

となり

$$f_*(\psi) = f \circ \psi = f \circ f_0^{-1} \circ \phi_0 = \phi,$$

すなわち $\phi \in \operatorname{Im} f_*$ が言えた.

(2) (g^* の単射性) $\phi \in \operatorname{Ker} g^* \Rightarrow \phi \circ g = 0 \Rightarrow \phi(g(M_2)) = 0 \overset{g(M_2)=M_3}{\Rightarrow} \phi(M_3) = 0 \Rightarrow \phi = 0.$

($\operatorname{Im} g^* \subset \operatorname{Ker} f^*$) $f^* \circ g^* = [\phi \mapsto \phi \circ g \circ f] \overset{g \circ f = 0}{=} 0.$

($\operatorname{Im} g^* \supset \operatorname{Ker} f^*$) $\phi \in \operatorname{Ker} f^* \Rightarrow \phi \circ f = 0 \Rightarrow \operatorname{Ker} \phi \supset \operatorname{Im} f \supset \operatorname{Ker} g \Rightarrow M_2/\operatorname{Ker} g \to M_2/\operatorname{Ker} \phi$ が well-defined. よって合成写像

$$[\psi \colon M_3 \overset{\overline{g}^{-1},\ \text{準同型定理}}{\cong} M_2/\operatorname{Ker} g \to M_2/\operatorname{Ker} \phi \overset{\overline{\phi},\ \text{準同型定理}}{\cong} \operatorname{Im} \phi \hookrightarrow N] \in \operatorname{Hom}_R(M_3, N)$$

が定義でき $g^*(\psi) = \phi$ を満たしている. □

問題 18. $R = \mathbb{Z}$ を考え, 系列

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$$

を考える. ただし $f\colon \mathbb{Z} \to \mathbb{Z}$ を $n \mapsto 2n$ で定める.

(1) $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$ は完全であることを示せ.

(2) $0 \to \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{f_*} \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{\pi_*} \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0$ は完全でないことを示せ.

(3) $0 \to \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{\pi^*} \mathrm{Hom}_R(\mathbb{Z}, \mathbb{Z}) \xrightarrow{f^*} \mathrm{Hom}_R(\mathbb{Z}, \mathbb{Z}) \to 0$ は完全でないことを示せ.

略解. (2) 上の命題より $\pi_*\colon \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$, $g \mapsto \pi \circ g$ の全射性以外は成立していることに注意. よって全射でないことを言えばよい. 実際 $\mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$ (零写像のみ), $\mathrm{Hom}_R(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \{0, \mathrm{id}\}$ が分かる.

(3) 同様に $f^*\colon \mathrm{Hom}_R(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_R(\mathbb{Z}, \mathbb{Z})$, $g \mapsto g \circ f$ が全射でないことを言えば良い. 例えば $(f^*g)(n) = g \circ f(n) = g(2n) = 2g(n)$ より $\mathrm{Im}\, f^* \subset \mathrm{Hom}_R(\mathbb{Z}, \mathbb{Z})$ は恒等写像を含まないことが分かる. □

定義 44. (1) M が <u>射影加群</u> であるとは

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0 \text{ が完全}$$
$$\Rightarrow 0 \to \mathrm{Hom}_R(M, M_1) \xrightarrow{f_*} \mathrm{Hom}_R(M, M_2) \xrightarrow{g_*} \mathrm{Hom}_R(M, M_3) \to 0 \text{ が完全}$$

が成り立つことである. 命題 43 よりこれは

$$L \xrightarrow{f} N \text{ が全射} \Rightarrow \mathrm{Hom}_R(M, L) \xrightarrow{f_*} \mathrm{Hom}_R(M, N) \text{ が全射}$$

とも言い換えられる. (M からの R-準同型写像は常に持ち上げが可能.)

(2) M が <u>入射加群</u> であるとは

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0 \text{ が完全}$$
$$\Rightarrow 0 \to \mathrm{Hom}_R(M_3, M) \xrightarrow{g^*} \mathrm{Hom}_R(M_2, M) \xrightarrow{f^*} \mathrm{Hom}_R(M_1, M) \to 0 \text{ が完全}$$

が成り立つことである. 命題 43 よりこれは

$$L \xrightarrow{f} N \text{ が単射} \Rightarrow \mathrm{Hom}_R(N, M) \xrightarrow{f_*} \mathrm{Hom}_R(L, M) \text{ が全射}$$

とも言い換えられる. (M への R-準同型写像の拡張が可能.)

11 射影加群, 入射加群 (2)

定理 45. 以下は同値.

(1) M は射影加群である.

(2) M はある自由加群の直和因子となる. すなわち

$$\exists \text{ 自由加群 } R^{\oplus B},\ \exists \text{左 } R\text{-加群 } M' \text{ s.t. } M \oplus M' \cong R^{\oplus B}.$$

証明. (2) $\Rightarrow$ (1) 問題 17 より

$$\mathrm{Hom}_R(M,L) \oplus \mathrm{Hom}_R(M',L) \cong \mathrm{Hom}_R(R^{\oplus B},L) \cong \prod_{b\in B} \mathrm{Hom}_R(R,L) \cong \prod_{b\in B} L.$$

ここで $\prod_{b\in B} L$ は L の $|B|$ 個の直積 ($|B|<\infty$ なら $= L^{\oplus B}$). $L \Rightarrow N$ でも同じであり

$$\begin{array}{ccc} \mathrm{Hom}_R(M,L) \oplus \mathrm{Hom}_R(M',L) & \cong & \prod_{b\in B} L \\ \downarrow & & \downarrow \\ \mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M',N) & \cong & \prod_{b\in B} N \end{array}$$

は可換図式となる. よって $L \to N$ が全射 $\overset{|B|=\infty \text{ なら選択公理が必要}}{\Rightarrow}$ $\prod_{b\in B} L \to \prod_{b\in B} N$ が全射 $\Rightarrow \mathrm{Hom}_R(M,L) \to \mathrm{Hom}_R(M,N)$ が全射, が言える.

(1) $\Rightarrow$ (2) M の生成系 B をとり, 写像

$$f\colon R^{\oplus B} \to M,\ (a_b)_{b\in B} \mapsto \sum_{b\in B} a_b b$$

を考える. 定理 17 での議論よりこれは全射 R-準同型. よって M が射影的なら

$$\mathrm{Hom}_R(M, R^{\oplus B}) \xrightarrow{f_*} \mathrm{Hom}_R(M,M)$$

も全射 R-準同型. とくに id_M へ移る $\phi \in \mathrm{Hom}_R(M, R^{\oplus B})$ が存在する. つまり

$$\exists \phi \in \mathrm{Hom}_R(M, R^{\oplus B}) \text{ s.t. } f_*(\phi) = f\circ\phi = \mathrm{id}_M.$$

このとき

$$M \oplus \mathrm{Ker}\, f \to R^{\oplus B},\ m \oplus x \mapsto \phi(m) + x$$

は同型となり, (1) が従う. 実際 R-準同型であることは自明であり

$$R^{\oplus B} \to M \oplus \mathrm{Ker}\, f,\ y \mapsto f(y) \oplus (y - \phi\circ f(y))$$

が逆写像を与えている. □

命題 46. $R = \mathbb{Z}$ の場合を考える. このとき $T := \mathbb{Q}/\mathbb{Z}$ は入射加群.

証明. 単射 R-準同型 $L \to N$ を考える. このとき像と L を同一視して, $L \subset N$ としても良い. 示すべきは

$$\phi \in \mathrm{Hom}_R(L, T) \Rightarrow \exists \Phi \in \mathrm{Hom}_R(N, T) \text{ s.t. } \Phi|_L = \phi.$$

ここで次の半順序集合を考える:

$$\{(M, \psi) \mid L \subset M \subset N,\ \psi \in \mathrm{Hom}_R(M, T),\ \psi|_L = \phi\},$$
$$(M, \psi) \preceq (M', \psi') \overset{\text{def}}{\Leftrightarrow} M \subset M',\ \psi'|_M = \psi.$$

これは帰納的半順序集合であることが言え, ツォルンの補題より極大元 (M, ψ) が存在する. このとき $M = N$ が言えれば ψ が題意を満たす.

$M = N$ は背理法で示す. もし $M \subsetneq N$ なら $N - M \ni n$ をとり

$$M' := M + \mathbb{Z}n,\ \psi' \colon M' \to T,\ m + kn \mapsto \psi(m) + k\psi'(n)$$

を矛盾なく定義できることを言えば, (M, ψ) が極大元であることに矛盾である. 実際

$$\psi'(n) := \begin{cases} \text{任意の元} \in T \text{ でよい} & (M \cap \mathbb{Z}n = \{0\}) \\ \psi(kn) = \frac{a}{b} \bmod \mathbb{Z} \text{ のとき } \frac{a}{kb} \bmod \mathbb{Z} & (M \cap \mathbb{Z}n = \mathbb{Z}kn) \end{cases}$$

とおけばよい. □

命題 47. (1) M を左 R-加群とする. 加法群は $\mathbb{Z}$-加群なので加法群 $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, T)$ が定まる. ここに R の右作用を

$$R \times M^* \to M^*,\ (r, \phi) \mapsto \phi r \colon M \to T,\ m \mapsto (\phi r)(m) := \phi(rm)$$

で定めることにより右 R-加群となる. また M が右 R-加群であれば $(r\phi)(m) := \phi(mr)$ により左 R-加群となる.

(2) 自然な写像

$$\iota_M \colon M \to (M^*)^*,\ m \mapsto [M^* \ni \phi \mapsto \phi(m) \in T] \in (M^*)^* = \mathrm{Hom}_{\mathbb{Z}}(M^*, T)$$

は単射 R-準同型写像となる.

(3) $\phi \colon L \to N$ が単射 R-準同型 $\Rightarrow$ $\phi^* \colon N^* \to L^*$, $f \mapsto f \circ \phi$ が全射 R-準同型.

(4) M が射影的 $\Rightarrow$ M^* が入射的.

証明. (1) は定義通り確かめればよい.

(2) R-準同型写像となるのは明らか. その核は

$$\{m \in M \mid \forall \phi \in M^*,\ \phi(m) = 0\}$$

となる. この核 $=\{0\}$, すなわち

$$m \neq 0 \Rightarrow \exists \phi \in M^* \text{ s.t. } \phi(m) \neq 0$$

を言えばよい. 実際 $t \in T$ を

$$t := \begin{cases} \frac{1}{l} \bmod \mathbb{Z} & (m \text{ の位数が } l < \infty \text{ のとき}) \\ 0 \text{ 以外の任意の元} & (m \text{ の位数が } \infty \text{ のとき}) \end{cases}$$

とおくと, M の部分 $\mathbb{Z}$-加群 $\mathbb{Z}m := \{km \mid k \in \mathbb{Z}\}$ に対し

$$\mathbb{Z}m \to T, \ km \mapsto kt$$

は $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}m, T)$ の元となる. T は入射加群だったので, この写像を拡張して $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, T)$ の元で m を $t \neq 0$ へ送るものが作れる.

(3) $\phi\colon L \to N$ が単射 R-準同型 $\Rightarrow \phi\colon L \to N$ が単射 $\mathbb{Z}$-準同型 $\overset{T \text{ は入射 } \mathbb{Z}\text{-加群}}{\Rightarrow} \phi^*\colon N^* \to L^*$ が全射 $\mathbb{Z}$-準同型. 一方で ϕ^* は R-準同型だったので題意を得る.

(4) 単射 R-準同型 $f\colon L \to N$ と $\phi \in \mathrm{Hom}_{\mathbb{R}}(L, M^*)$ に対し

$$\Phi \in \mathrm{Hom}_{\mathbb{R}}(N, M^*) \text{ s.t. } \Phi \circ f = \phi$$

を構成すればよい. $\phi^* \in \mathrm{Hom}_{\mathbb{R}}((M^*)^*, L^*)$ と自然な写像 $\iota_M\colon M \to (M^*)^*$ との合成

$$\phi^* \circ \iota_M\colon M \overset{\iota_M}{\to} (M^*)^* \overset{\phi^*}{\to} L^*$$

に M が入射的であることを使うと ((3) より $f^* \in \mathrm{Hom}_{\mathbb{R}}(N^*, L^*)$ は全射に注意)

$$\exists F\colon M \to N^* \text{ s.t. } f^* \circ F = \phi^* \circ \iota_M.$$

さらに合成写像

$$\Phi := F^* \circ \iota_N\colon N \overset{\iota_N}{\to} (N^*)^* \overset{F^*}{\to} M^*$$

を考えると, これが求めるものである. $\square$

定理 48. 任意の R-加群は入射加群の部分加群 (と同型) になる.

証明. M を任意の R-加群とする. M^* の生成系 B をとり, 全射 R-準同型

$$f\colon R^{\oplus B} \to M^*, \ (a_b)_{b \in B} \mapsto a_b b$$

を考える. このとき $f^*\colon (M^*)^* \to (R^{\oplus B})^*$ は単射 R-準同型. これと $\iota_M\colon M \to (M^*)^*$ の合成より, 単射 R-準同型

$$f^* \circ \iota_M\colon M \to (R^{\oplus B})^*$$

を得る. $R^{\oplus B}$ は自由加群だから射影的. よって $(R^{\oplus B})^*$ は入射的なので題意を得る. $\square$

問題 19. M を任意の R-加群とする.

(1) $0 \leftarrow M \leftarrow P_0 \leftarrow P_1 \leftarrow P_2 \leftarrow \cdots$ が完全列となるような射影加群 $P_0, P_1, \ldots$ が取れる. このような完全列を M の **射影的分解** と呼ぶ.

(2) $0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$ が完全列となるような入射加群 $I^0, I^1, \ldots$ が取れる. このような完全列を M の **入射的分解** と呼ぶ.

略解. (1) 定理 45 の証明中のように, M の生成系 B_0 をとって全射 R-準同型 $f_0\colon R^{\oplus B_0} \to M$ を作る. この核 $\operatorname{Ker} f_0$ の生成系 B_1 にも同様に全射 R-準同型 $f_1\colon R^{\oplus B_1} \to \operatorname{Ker} f_0$ が作れる. これを続けて $0 \leftarrow M \xleftarrow{f_0} R^{\oplus B_0} \xleftarrow{f_1} R^{\oplus B_1} \leftarrow \cdots$ が求めるもの.

(2) 上の定理より $0 \to M \xrightarrow{f_0} I^0$ まで作れる. 同様に剰余加群 $I_0/\operatorname{Im} f_0$ に対して $0 \to I_0/\operatorname{Im} f_0 \xrightarrow{f_1} I^1$ を作り, 射影 $\pi\colon I_0 \to I_0/\operatorname{Im} f_0$ との合成 $I_0 \to I_1$ を考えて $0 \to M \xrightarrow{f_0} I^0 \xrightarrow{f_1 \circ \pi} I^1 \to \cdots$ と続ければよい. $\square$

12 テンソル積

注意

この講義では簡単のため R を可換環とする．実際は非可換環の場合でも テンソル積 は定義できる．

定義 49. L, M, N を R-加群とする．写像

$$\phi\colon M \times N \to L$$

が R-双線形写像 であるとは，任意の $r \in R$, $m, m' \in M$, $n, n' \in N$ に対して

$$\begin{aligned}
\phi(rm, n) &= \phi(m, rn) = r\phi(m, n), \\
\phi(m + m', n) &= \phi(m, n) + \phi(m', n), \\
\phi(m, n + n') &= \phi(m, n) + \phi(m, n')
\end{aligned}$$

が成り立つことである．

定理 50. M, N を R-加群とする．このとき R-加群 T と R-双線形写像 $\tau\colon M \times N \to T$ の組で以下の「性質」を満たすものが存在する．

「性質」 任意の R-加群 L と R-双線形写像 $\phi\colon M \times N \to L$ に対し，
R-準同型写像 $f\colon T \to L$ で $\phi = f \circ \tau$ を満たすものがただ一つ存在する．

さらにこの「性質」を満たすものは，以下の意味で同型を除いて唯一つ存在する．

$\tau\colon M \times N \to T$, $\tau'\colon M \times N \to T'$ が「性質」を満たせば，
R-同型写像 $g\colon T \to T'$ で $g \circ \tau = \tau'$ となるものが存在する．

この T を M, N の R 上の テンソル積 と呼び，記号 $M \otimes_R N$ で表す．また像 $\tau(m, n)$ を $m \otimes n \in M \otimes_R N$ で表す．

問題 20. 自由加群 $R^{\oplus B}, R^{\oplus C}$ (B, C はそれぞれの基底) のテンソル積は

$$\tau\colon R^{\oplus B} \times R^{\oplus C} \to R^{\oplus B \times C},\ (\sum_{b \in B} r_b b, \sum_{c \in C} r_c c) \mapsto \sum_{(b,c) \in B \times C} r_b r_c (b, c)$$

で与えられることを確かめよ．(上記の「性質」を満たすことを示せ.) とくに $R^m \otimes_R R^n \cong R^{mn}$ である．

略解. τ が R-双線形写像であることは明らかであろう．R-双線形写像 $\phi\colon R^{\oplus B} \times R^{\oplus C} \to L$ が存在したとする．このとき

- $f\colon R^{\oplus B \times C} \to L$, $\sum_{(b,c) \in B \times C} r_{(b,c)}(b, c) \mapsto \sum_{(b,c) \in B \times C} r_{(b,c)} \phi(b, c)$ は R-準同型写像であり $\phi = f \circ \tau$ を満たす．

- R-準同型写像 $g\colon R^{\oplus B\times C}\to L$ も $\phi=g\circ\tau$ を満たせば $f=g$.

を言えばよい. 実際 f が R-準同型写像は明らかであり,

$$f\circ\tau\left((\sum_{b\in B}r_b b,\sum_{c\in C}r_c c)\right)=f\left(\sum_{(b,c)\in B\times C}r_b r_c(b,c)\right)=\sum_{(b,c)\in B\times C}r_b r_c\phi(b,c)$$

は, ϕ が R-双線形写像であることから

$$\phi(\sum_{b\in B}r_b b,\sum_{c\in C}r_c c)$$

と一致する. 後半は

$$\begin{aligned}f\circ\tau=\phi=g\circ\tau&\Rightarrow\forall b\in B,c\in C,\ f\circ\tau(b,c)=g\circ\tau(b,c)\\&\Rightarrow\forall b\in B,c\in C,\ f(b,c)=g(b,c)\end{aligned}$$

となり, 任意の基底 $\in B\times C$ の行き先が一致するので $f=g$ となる. □

定理 *50* の証明の概略.

- $\mathcal{T}:=R^{\oplus M\times N}$: 積集合 $M\times N$ を基底とする自由 R-加群.
- $\mathcal{N}:=\sum_{m,m'\in M,\ n\in N}R((m+m',n)-(m,n)-(m',n))+\sum_{m,\in M,\ n\in N,r\in R}R((rm,n)-r(m,n))$
  $+\sum_{m,\in M,\ n,n'\in N}R((m,n+n')-(m,n)-(m,n'))+\sum_{m,\in M,\ n\in N,r\in R}R(r(m,n)-(m,rn))$
  : $(m+m',n)-(m,n)-(m',n),\dots$ の形の元 $\in\mathcal{T}$ で生成される部分加群.
- $T:=\mathcal{T}/\mathcal{N}$: 剰余加群.
- $\tau\colon M\times N\to T,\ (m,n)\mapsto(m,n)+\mathcal{N}$.

  とおけば題意を満たす. □

注意 51. (構成方法より) 以下が分かる. $m,m'\in M$, $n,n'\in N$, $r\in R$ に対し

$$\begin{aligned}&(m+m')\otimes n=m\otimes n+m'\otimes n,\ m\otimes(n+n')=m\otimes n+m\otimes n',\\&(rm)\otimes n=m\otimes(rn)=r(m\otimes n).\end{aligned}$$

とくに

$$0_M\otimes n=m\otimes 0_N=0_R(m\otimes n)=0_{M\otimes_R N}$$

に注意.

命題 52. (1) テンソル積 $M\otimes_R N$ の一般元は $\sum_{i=1}^k m_i\otimes n_i$ $(k\geq 0,\ m\in M,\ n\in N)$ の形で書ける. (ただしこの表記は一意的ではない.)

(2) R-準同型写像 $f\colon M\to M'$, $g\colon N\to N'$ に対して

$$f\otimes g\colon M\otimes_R N\to M'\otimes_R N',\ \sum_{i=1}^{k} m_i\otimes n_i\mapsto \sum_{i=1}^{k} f(m_i)\otimes g(n_i)$$

を満たす R-準同型写像がただ一つ存在する.

(3) 直和とテンソル積は “分配法則” を満たす: $\left(\bigoplus_{i\in I} M_i\right)\otimes_R N\cong\bigoplus_{i\in I}(M_i\otimes_R N)$.

(4) $R^{\oplus B}\otimes_R M\cong M^{\oplus B}$ ($M^{\oplus B}$ は M の $|B|$ 個の直和). とくに $R^{\oplus B}\otimes_R M$ の元は $\sum_{b\in B} b\otimes m_b$ ($m_b\in M$, 有限個を除いて $=0$) の形に一意的に書ける.

証明. (1) は上記の $M\otimes_R N$ の構成方法より明らか.

(2) $M\times N\to M'\otimes_R N'$, $(m,n)\mapsto f(m)\otimes f(n)$ は明らかに R-双線形写像. よってテンソル積の定義より $\exists! M\otimes_R N\to M'\otimes_R N'$ s.t. $m\otimes n\mapsto f(m)\otimes f(n)$.

(3) R-双線形写像 $\left(\bigoplus_{i\in I} M_i\right)\times N\to\bigoplus_{i\in I}(M_i\otimes_R N)$, $(\sum_{i\in I} m_i, n)\mapsto\sum_{i\in I}(m_i\otimes n)$ が引き起こす写像

$$f\colon \left(\bigoplus_{i\in I} M_i\right)\otimes_R N\to\bigoplus_{i\in I}(M_i\otimes_R N),\ (\sum_{i\in I} m_i)\otimes, n\mapsto\sum_{i\in I}(m_i\otimes n)$$

が同型写像を与える. 実際, 逆写像が以下の手順で構成できる: R-双線形写像 $M_i\times N\to\left(\bigoplus_{i\in I} M_i\right)\otimes_R N$, $(m_i,n)\mapsto m_i\otimes n$ が引き起こす写像

$$g_i\colon M_i\otimes_R N\to\left(\bigoplus_{i\in I} M_i\right)\otimes_R N,\ m_i\otimes n\mapsto m_i\otimes n$$

の直和

$$\bigoplus_{i\in I} g_i\colon\bigoplus_{i\in I}(M_i\otimes_R N)\to\left(\bigoplus_{i\in I} M_i\right)\otimes_R N,\ \sum_{i\in I} m_i\otimes n\mapsto(\sum_{i\in I} m_i)\otimes n.$$

(4) (3) より $R\otimes_R M\cong M$ を言えばよい. 実際 R-双線形写像 $R\times M\to M$, $(r,m)\mapsto rm$ が引き起こす写像

$$R\otimes_R M\to M,\ r\otimes m\mapsto rm$$

と

$$M\to R\otimes_R M,\ m\mapsto 1\otimes m$$

が互いに逆写像になっている. □

命題 53. 任意の R-加群 M_1, M_2, M_3, N に対し以下が成り立つ.

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0 \text{ が完全} \Rightarrow M_1 \otimes_R N \overset{f\otimes \mathrm{id}_N}{\to} M_2 \otimes_R N \overset{g\otimes \mathrm{id}_N}{\to} M_3 \otimes_R N \to 0 \text{ が完全}.$$

証明. 命題 52-(1) を使って具体的に写像を書けば $g \otimes \mathrm{id}_N$ の全射性と $\mathrm{Im}\, f \otimes \mathrm{id}_N \subset \mathrm{Ker}\, g \otimes \mathrm{id}_N$ が言える. ここでは $\mathrm{Im}\, f \otimes \mathrm{id}_N \supset \mathrm{Ker}\, g \otimes \mathrm{id}_N$ のみ示す. g は全射なので, M_3 の任意の元は $g(m)$ $(m \in M_2)$ の形に書ける. このとき R-双線形写像

$$\phi\colon M_3 \times N \to (M_2 \otimes_R N)/\mathrm{Im}\, f \otimes \mathrm{id}_N,\ (g(m), n) \mapsto m \otimes n \bmod \mathrm{Im}\, f \otimes \mathrm{id}_N$$

が矛盾なく定まる. 実際

$$\begin{aligned} g(m) = g(m') &\Rightarrow m - m' \in \mathrm{Ker}\, g = \mathrm{Im}\, f \\ &\Rightarrow m \otimes n - m' \otimes n = (m - m') \otimes n \in \mathrm{Im}\, f \otimes \mathrm{id}_N \end{aligned}$$

である. よって, この ϕ から定まる R-準同型写像

$$\Phi\colon M_3 \otimes_R N \to (M_2 \otimes_R N)/\mathrm{Im}\, f \otimes \mathrm{id}_N,\ g(m) \otimes n \mapsto m \otimes n \bmod \mathrm{Im}\, f \otimes \mathrm{id}_N$$

が考えられる. よって

$$\begin{aligned} &\sum_i m_i \otimes n_i \in \mathrm{Ker}\, g \otimes \mathrm{id}_N \Rightarrow \sum_i g(m_i) \otimes n_i = 0 \\ &\Rightarrow \Phi(\sum_i g(m_i) \otimes n_i) = \sum_i \Phi(g(m_i) \otimes n_i) = \sum_i m_i \otimes n_i \bmod \mathrm{Im}\, f \otimes \mathrm{id}_N = 0 \\ &\Rightarrow \sum_i m_i \otimes n_i \in \mathrm{Im}\, f \otimes \mathrm{id}_N \end{aligned}$$

が言えた. □

問題 21. $R = M_1 = \mathbb{Z}$, $M_2 = \mathbb{Q}$ と自然な単射 $0 \to \mathbb{Z} \to \mathbb{Q}$ を考える. このとき $N = \mathbb{Z}/2\mathbb{Z}$ に対して

$$0 \to \mathbb{Z} \otimes_Z \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q} \otimes_Z \mathbb{Z}/2\mathbb{Z}$$

は成り立たないことを確かめよ.

略解. $\mathbb{Z} \otimes_Z \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ であった. 一方で $\mathbb{Q} \otimes_Z \mathbb{Z}/2\mathbb{Z} = 0$ (零元のみからなる加群) が言える. 実際 $\mathbb{Q} \otimes_Z \mathbb{Z}/2\mathbb{Z}$ の一般元は $\frac{a}{b} \otimes \overline{c}$ $(a, b, c \in \mathbb{Z})$ の形の元の一次結合で書かれ,

$$\frac{a}{b} \otimes \overline{c} = (2 \cdot \frac{a}{2b}) \otimes \overline{c} = \frac{a}{2b} \otimes (2 \cdot \overline{c}) = \frac{a}{2b} \otimes \overline{0} = 0$$

となる. □

定義 54. R-加群 N が <u>平坦</u> であるとは, 任意の R-加群 M_1, M_2 に対し以下が成り立つことである.

$$0 \to M_1 \xrightarrow{f} M_2 \text{ が完全} \Rightarrow 0 \to M_1 \otimes_R N \overset{f\otimes \mathrm{id}_N}{\to} M_2 \otimes_R N \text{ が完全}.$$

定理 55. 射影加群は平坦である.

証明. N を射影加群とする. このとき N はある自由加群 $R^{\oplus B}$ の直和因子であった (正確には同一視できる). すなわち

$$M \oplus N = R^{\oplus B}$$

としてよい. このとき

$$f\colon M_1 \to M_2 \text{ が単射} \Rightarrow f^{\oplus B}\colon M_1^{\oplus B} \to M_2^{\oplus B} \text{ が単射},$$

が言える, さらに可換図式

$$\begin{array}{ccc}
M_1^{\oplus B} & \xrightarrow{f^{\oplus B}} & M_2^{\oplus B} \\
\wr\| & & \wr\| \\
M_1 \otimes_R R^{\oplus B} & \xrightarrow{f \otimes \mathrm{id}_{R^{\oplus B}}} & M_2^{\oplus B} \otimes_R R^{\oplus B} \\
\wr\| & & \wr\| \\
M_1 \otimes_R N \oplus M_1 \otimes_R M & \xrightarrow{f \otimes \mathrm{id}_N \oplus f \otimes \mathrm{id}_M} & M_2 \otimes_R N \oplus M_2 \otimes_R M \\
\uparrow & & \uparrow \\
M_1 \otimes_R N & \xrightarrow{f \otimes \mathrm{id}_N} & M_2 \otimes_R N
\end{array}$$

を考える. ここで縦の $\wr\|$ は命題 52-(3), (4) より従う. このとき $f \otimes \mathrm{id}_N$ は単射 $f^{\oplus B}$ の制限とみなせるので単射である. $\square$

13　ネター加群, アルチン加群

定義 56. M を左 R-加群とする. (右でも同様である.)

(1) M が <u>ネター加群</u> であるとは, 任意の部分加群の増大列

$$M_1 \subset M_2 \subset \cdots \subset M_i \subset \cdots \subset M$$

に対して, ある n が存在して $M_n = M_{n+1} = \cdots$ となることである.

(2) M が <u>アルチン加群</u> であるとは, 任意の部分加群の減少列

$$M \supset M_1 \supset M_2 \supset \cdots \supset M_i \supset \cdots$$

に対して, ある n が存在して $M_n = M_{n+1} = \cdots$ となることである.

命題 57. (1) 以下は同値である.

- (a) M はネター加群である.
- (b) M の部分加群からなる空でない任意の集合族は, 包含関係に関して極大元を持つ.
- (c) M の任意の部分加群は有限生成である.

(2) 以下は同値である.

- (a) M はアルチン加群である.
- (b) M の部分加群からなる空でない任意の集合族は, 包含関係に関して極小元を持つ.

証明. ネター環の定義 (定義 29) の同値性の証明 (堀田良之著「代数入門 –群と加群–」裳華房, 命題 9.6, p50 参照) と同様なので省略. □

注意 58. 環 R 自体を左 R-加群とみなしたとき, $I \subset R$ が左イデアルであるとこと, 部分加群であることは同値である. よって以下が分かる. (右でも同じ.)

(1) 環 R が左ネター環であることと, 左 R-加群としてネター加群であることは同値.

(2) 環 R が左アルチン環であることと, 左 R-加群としてアルチン加群であることは同値.

定理 59. 左 R-加群の短完全列

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

を考える. このとき

(1) M_2 がネター加群 $\Leftrightarrow$ M_1, M_3 がネター加群.

(2) M_2 がアルチン加群 $\Leftrightarrow$ M_1, M_3 がアルチン加群.

右加群でも同様である.

証明. ネター性もアルチン性も同じ証明なので, 前者のみ示す.

($\Rightarrow$) $M_1 \subset M_2$ とみなせるので, M_1 の部分加群は M_2 の部分加群とみなせる. よって M_1 の部分加群の増大列

$$N_1 \subset N_2 \subset \cdots \subset N_i \subset \cdots \subset M_1$$

は M_2 の部分加群の増大列

$$N_1 \subset N_2 \subset \cdots \subset N_i \subset \cdots \subset M_1 \subset M_2$$

でもあり, M_2 のネター性より, ある n で止まる. つぎに M_3 の部分加群の増大列

$$N_1 \subset N_2 \subset \cdots \subset N_i \subset \cdots \subset M_3$$

を考える. 部分加群の逆像は部分加群になるから, M_2 の部分加群の増大列

$$g^{-1}(N_1) \subset g^{-1}(N_2) \subset \cdots \subset g^{-1}(N_i) \subset \cdots \subset M_2$$

を得る. このときやはり, M_2 のネター性より, ある n で止まる:

$$g^{-1}(N_n) = g^{-1}(N_{n+1}) = \cdots .$$

g の全射性より $g(g^{-1}(N_i)) = N_i$ であることに注意して $N_n = N_{n+1} = \cdots$ を得る.

($\Leftarrow$) M_2 の部分加群の増大列

$$N_1 \subset N_2 \subset \cdots \subset N_i \subset \cdots \subset M_2$$

に対して, M_1, M_3 の部分加群の増大列

$$\begin{aligned} &f^{-1}(N_1) \subset f^{-1}(N_2) \subset \cdots \subset f^{-1}(N_i) \subset \cdots \subset M_1, \\ &g(N_1) \subset g(N_2) \subset \cdots \subset g(N_i) \subset \cdots \subset M_3 \end{aligned}$$

を考える. M_1, M_3 のネター性よりこれらはいずれ止まり, より大きい n を考えることにより

$$f^{-1}(N_n) = f^{-1}(N_{n+1}) = \cdots , \ g(N_n) = g(N_{n+1}) = \cdots$$

となる. 一般論として

- $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ が完全
  $\Rightarrow$ 部分加群 $B_0 \subset B$ に対して $0 \to f^{-1}(B_0) \xrightarrow{f} B_0 \xrightarrow{g} g(B_0) \to 0$ が完全.

が成り立つので, 完全系列の可換図式

$$
\begin{array}{ccccccccc}
0 & \to & f^{-1}(N_n) & \to & N_n & \to & g(N_n) & \to & 0 \\
 & & \| & & \cap & & \| & & \\
0 & \to & f^{-1}(N_{n+1}) & \to & N_{n+1} & \to & g(N_{n+1}) & \to & 0
\end{array}
$$

を得る. 再び一般論として

- $\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \| & & \cap & & \| & & \\ 0 & \to & X & \to & Y & \to & Z & \to & 0 \end{array}$ か完全系列の可換図式 $\Rightarrow B = Y$.

が成り立つので $N_n = N_{n+1} = \cdots$ を得る. □

問題 22. 上記の一般論を示せ. ただし, 簡単のため以下の状況で考えよ. B の部分加群 A に対して, 自然な完全列 $0 \to A \xrightarrow{i} B \xrightarrow{\pi} B/A \to 0$ を考える.

(1) 任意の部分加群 $B_0 \subset B$ に対して, 制限 $0 \to A \cap B_0 \xrightarrow{i|_{A\cap B_0}} B_0 \xrightarrow{\pi|_{B_0}} B_0/(A \cap B_0) \to 0$ も完全系列となる.

(2) 完全系列の可換図式

$$
\begin{array}{ccccccccc}
0 & \to & A \cap B_0 & \to & B_0 & \to & B_0/(A \cap B_0) & \to & 0 \\
 & & \cap & & \cap & & \psi\downarrow & & \\
0 & \to & A & \to & B & \to & B/A & \to & 0
\end{array}
$$

を考える. ただし ψ は自然な写像 $b \bmod (A \cap B_0) \mapsto b \bmod A$ とする. このとき

$$B = B_0 \Leftrightarrow A = A \cap B_0, B_0/(A \cap B_0) \overset{\psi}{\cong} B/A$$

略解. (1) i は単射なので, その制限 $i|_{A\cap B_0}$ も単射. $\pi|_{B_0}\colon B_0 \to B_0/(A \cap B_0)$ の全射性は明らか. 残りの

$$\operatorname{Im} i|_{A\cap B_0} = i(A \cap B_0) = A \cap B_0 = [\operatorname{Ker} \pi|_{B_0}\colon B_0 \to B_0/(A \cap B_0)]$$

も明らかであろう.

(2) $B = B_0$ なら上下の完全列は同じものなので ($\Rightarrow$) は明らかであろう. ($\Leftarrow$) は $A = A \cap B_0$ なら $\psi\colon B_0/A \cong B/A$ なので $B = B_0$ が言える. □

定理 60. 左ネター環 R 上の有限生成左 R-加群はネター加群. なお, 左を右に, または, ネターをアルチンにしても成立する (4 通り).

証明. 左ネター性の場合の示す. (他 3 通りも同様である.) M が n 元生成

$$M = \sum_{i=1}^{n} Rm_i$$

であるとし, n に関する帰納法を用いる. $n=1$ のとき

$$\phi\colon R \to M,\ r \mapsto rm_1$$

は全射 R-準同型なので, 完全列

$$0 \to \operatorname{Ker}\phi \to R \xrightarrow{\phi} M \to 0$$

を得る. よって定理 59 より [R が左ネーター環 $\Rightarrow$ M がネーター加群] が言える.

次に $1 \sim n-1$ まで成立すると仮定して n の場合を考える. 部分加群 $N := \sum_{i=1}^{n-1} Rm_i$ と剰余加群 $\overline{M} := M/N$, 自然な射影 $M \to \overline{M}$, $m \mapsto \overline{m} := m + N$ を考えると, 完全列

$$0 \to N \to M \to \overline{M} \to 0$$

を得る. このとき N は $n-1$ 元生成, $\overline{M}$ は 1 元生成である ($\star$) ことに注意すると, 帰納法の仮定より $N, \overline{M}$ はネーター加群で, 再び定理 59 より題意が従う.

($\star$) は以下のように考えればわかる: $\overline{M}$ の一般元は

$$\overline{M} = \left\{ \overline{\textstyle\sum_{i=1}^{n} r_i m_i} \mid r_1, \ldots, r_n \in R \right\}$$

と書ける. このとき $m_1, \ldots, m_{n-1} \in N$ より $\overline{m_1}, \ldots, \overline{m_{n-1}} = 0$ だから $\overline{\sum_{i=1}^{n} r_i m_i} = r_n \overline{m_n}$ となる. よって

$$\overline{M} = \{ r\overline{m_n} \mid r \in R \} = R\overline{m_n}$$

であり, 1 元生成. □

ある加群 M を調べようとおもったとき, そのネター性, アルチン性は, 重要な性質となる. (例えばネーター加群であれば, 有限生成であることが保証されるので “便利” である.) 上の定理より, ある環 R がネタ一環またはアルチン環であれば, 任意の R-加群がネター性またはアルチン性を持つことになり, やはり重要な性質であることが分かる.

以下, 参考のため, ネタ一環, アルチン環に関する便利な命題, 定理を, 証明なしに並べて置く. 詳しくは, 堀田良之著「代数入門 –群と加群–」裳華房, p144- などを参照.

命題 61. 左ネーター環の剰余環も左ネーター環となる. なお, 左を右に, または, ネーターをアルチンにしても成立する (4 通り).

定理 62 (ヒルベルトの基本定理)**.** 可換ネーター環上有限生成な可換環はネーター環である.

注意 63. 体は PID なので, とくに可換ネーター環であった. よって上の定理と命題より,

- 体 K 係数の n 変数多項式環 $K[X_1, \ldots, X_n]$.
- さらに剰余環 $K[X_1, \ldots, X_n]/I$.

などは可換ネーター環となる. また, 体係数でなくても, 可換ネーター環 R を係数とすれば同じことが言える.

定理 64. 左アルチン環は左ネーター環である. (右でも同様.)

14　先進的な話題：Ext 函手, 群コホモロジー, Hilbert 90

この節は講義時間が余っていたとき用. テストなどには出さない.

私の専門 (整数論) に関連して, 群コホモロジー, Hilbert の定理 90, そして, ディオファントス方程式の整数解への応用を紹介する. 内容が広範囲になるため, 正確性より雰囲気を重視する.

ピタゴラス数

整数係数多項式 $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ を用いて書かれる方程式

$$F(x_1, \dots, x_n) = 0$$

のことを <u>ディオファントス方程式</u> とよぶ. とくに整数論では, ディオファントス方程式の整数解, 有理数解を探すことが重要視される. 例えば [3 辺の長さが整数となる直角三角形] を求めることは

$$x^2 + y^2 = z^2$$

の整数解 (<u>ピタゴラス数</u>) を求めることになり, ディオファントス方程式の一例とみなせる. また, これは

$$x^2 + y^2 = 1$$

の有理数解を求めることと同値である.

導来関手

(必ずしも全てではなく, 一部の) 加法群 A に対して別の加法群 $F(A)$ を与えるルール F で "良い性質" をもつものを <u>関手</u> と呼ぶ. 加法群全体 $\mathcal{C}$ と, その部分集合 $\mathcal{C}_0$ を考えて, 写像

$$F\colon \mathcal{C}_0 \to \mathcal{C}$$

を考えている感じである. "良い性質" には以下も含まれる: (一部の) $A, B \in \mathcal{C}_0$ と, (一部の) 準同型 $f\colon A \to B$ に対して, 準同型

$$F(f)\colon F(A) \to F(B)$$

も定まる.

関手 F が, さらに

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \text{ が完全} \Rightarrow 0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \text{ が完全}$$

を満たすとき, F は 左完全 である, という. 例えば R-加群全体 $\mathcal{C}_R$ を考えると

$$\begin{aligned}
&F\colon \mathcal{C}_R \to \mathcal{C},\ A \mapsto \mathrm{Hom}_R(M, A),\\
&f\colon A \to B \Rightarrow F(f) := f_*\colon \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B),\ \phi \mapsto f \circ \phi
\end{aligned}$$

は左完全関手である (命題 43-(1)).

左完全関手 $F\colon \mathcal{C}_0 \to \mathcal{C}$ を考える. このとき, 考えている C_0 が "充分単射的" であれば, F に付随した別の関手

$$R^n F\colon \mathcal{C}_0 \to \mathcal{C}\ (n = 1, 2, 3, \dots)$$

で

$$\begin{aligned}
&0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0 \text{ が完全}\\
\Rightarrow\ &0 \to \quad F(A) \quad \xrightarrow{F(f)} \quad F(B) \quad \xrightarrow{F(g)} \quad F(C)\\
&\xrightarrow{\delta} R^1F(A) \xrightarrow{R^1F(f)} R^1F(B) \xrightarrow{R^1F(g)} R^1F(C)\\
&\xrightarrow{\delta} R^2F(A) \xrightarrow{R^2F(f)} R^2F(B) \xrightarrow{R^2F(g)} R^2F(C)\\
&\xrightarrow{\delta} \cdots \text{ が完全}
\end{aligned}$$

を満たすものが構成できる (正確には, 準同型 $\delta\colon R^nF(C) \to R^{n+1}(A)$ 達も同時に構成される). この関手 R^nF を F の 右導来関手, 後半の完全列を F から 誘導される長完全列 と呼ぶ. (ちなみに, この R は right から来ており, 環 R とは関係ない.) 例えば, R-加群全体 $\mathcal{C}_R$ が "充分単射的" であるとは, 各 R-加群 M が入射的分解をもつことである. 特に, 問題 19-(2) より $\mathcal{C}_R$ は充分入射的で, 左完全関手 $F = \mathrm{Hom}_R(M,\ )$ は右導来関手を持つ.

定義 65. $\mathrm{Hom}_R(M,\ )$ の右導来関手は Ext 関手 と呼ばれ $\mathrm{Ext}^n_R(M,\ ) := R^n\mathrm{Hom}_R(M,\ )$ で表される. 具体的には

$$\mathrm{Ext}^n_R(M,\ )\colon N \mapsto \mathrm{Ext}^n_R(M, N)$$

は以下の手順で構成される:

- N の入射的分解 $0 \to N \xrightarrow{i_0} I^0 \xrightarrow{i_1} I^1 \xrightarrow{i_2} I^2 \to \cdots$ を一つとる.
- 関手 $\mathrm{Hom}_R(M,\ )$ により, 系列

$$0 \to \mathrm{Hom}_R(M, N) \xrightarrow{i_{0*}} \mathrm{Hom}_R(M, I^0) \xrightarrow{i_{1*}} \mathrm{Hom}_R(M, I^1) \xrightarrow{i_{2*}} \mathrm{Hom}_R(M, I^2) \to \cdots$$

  を得る. 左完全性より第 4 項までは完全であるが, それ以降は完全とは限らない.

- $i_{k+1} \circ i_k = 0$ より $i_{k+1*} \circ i_{k*} = 0$, すなわち $\operatorname{Im} i_{k*} \subset \operatorname{Ker} i_{k+1*}$ が分かる. ここで

$$\operatorname{Ext}^n_R(M, N) := \begin{cases} \operatorname{Ker} i_{n+1*}/\operatorname{Im} i_{n*} & (n \geq 1) \\ \operatorname{Ker} i_{1*} & (n = 0) \end{cases}$$

とおく (この定義は入射的分解の取り方によらないことが示せる). 第 4 項までの完全性より $\operatorname{Ext}^0_R(M, N) := \operatorname{Ker} i_{1*} = \operatorname{Im} i_{0*} \cong \operatorname{Hom}_{\mathbb{R}}(M, N)$ に注意.

注意 66. $\operatorname{Ext}^n_R(M, N)$ は M の射影的分解 $0 \leftarrow M \overset{p_0}{\leftarrow} P_0 \overset{p_1}{\leftarrow} P_1 \overset{p_2}{\leftarrow} P_2 \leftarrow \cdots$ を使っても, 同様に構成できる.

問題 23. Ext 関手は実際に "計算" できるもので, その計算によって様々なことが分かる. 例えば以下を確かめてみよ.

(1) N が入射的であれば $0 \to N \overset{\mathrm{id}}{\to} N \to 0 \to 0 \to \cdots$ は入射分解を与える.

(2) (1) の入射分解に関手 $\operatorname{Hom}_R(M, \ )$ を施した系列を書け.

(3) $\operatorname{Ext}^n_R(M, N) = 0$ $(n \geq 1)$ を確かめよ.

(4) 逆に, 任意の M に対して $\operatorname{Ext}^1_R(M, N) = 0$ であれば, N は入射的であることを説明せよ. ($\operatorname{Hom}_R(M, \ )$ から誘導される長完全列を書いてみよ.)

略解. (2) $0 \to \operatorname{Hom}_R(M, N) \overset{\mathrm{id}}{\to} \operatorname{Hom}_R(M, N) \to 0 \to 0 \to \cdots$.

(3) $\operatorname{Ext}^n_R(M, N) = 0/0 = 0$.

(4) $0 \to M_1 \to M_2 \to M_3 \to 0$ が完全
$\Rightarrow 0 \to \operatorname{Hom}_R(M, M_1) \to \operatorname{Hom}_R(M, M_2) \to \operatorname{Hom}_R(M, M_3) \to \operatorname{Ext}^1_R(M, M_1) \to \cdots$ が完全. さらに $\operatorname{Ext}^1_R(M, M_1) = 0$
$\Rightarrow 0 \to \operatorname{Hom}_R(M, M_1) \to \operatorname{Hom}_R(M, M_2) \to \operatorname{Hom}_R(M, M_3) \to 0$. □

群コホモロジー

定義 67. G を (可換群とは限らない) 群とし, その単位元を e で表す. ここでは簡単のため G は有限群とする. また M を加法群とする.

(1) 群 G の加法群 M への <u>作用</u> とは, 写像

$$\cdot : G \times M \to M, \ (g, m) \mapsto gm$$

で $em = m$, $g(hm) = (gh)m$, $g(m + m') = gm + gm'$ $(g, h \in G,\ m, m' \in M)$ を満たすもののことである.

(2) 群 G が加法群 M に作用しているとき, G-不変部分 を

$$M^G := \{m \in M \mid \forall g \in G,\ gm = m\}$$

で定める. これは M の部分加法群となる.

(3) $\mathbb{Z}$ 上の 群環 $\mathbb{Z}[G]$ を

$$\begin{aligned}
&\mathbb{Z}[G] := \{\sum_{g \in G} n_g g \mid n_g \in \mathbb{Z}\}, \\
&\sum_{g \in G} m_g g + \sum_{g \in G} n_g g := \sum_{g \in G} (m_g + n_g) g, \\
&\left(\sum_{g \in G} m_g g\right)\left(\sum_{g \in G} n_g g\right) := \sum_{g \in G}\left(\sum_{h \in G} m_h n_{h^{-1}g}\right) g
\end{aligned}$$

で定める. (加法群としては $\mathbb{Z}$ 上 G で生成される自由加群. これに自然な掛け算を定義した.) 群環 $\mathbb{Z}[G]$ は環となる.

(4) 群 G が加法群 M に作用しているとき

$$\left(\sum_{g \in G} n_g g\right) m := \sum_{g \in G} n_g (gm)$$

により M は左 $\mathbb{Z}[G]$-加群となる.

(5) とくに, 群 G の $M := \mathbb{Z}$ への自明な作用

$$G \times \mathbb{Z} \to \mathbb{Z},\ (g, n) \mapsto n$$

を考え, (自明な) $\mathbb{Z}[G]$-加群 $\mathbb{Z}$ を定義する.

定義 68. 群 G が加法群 M へ作用しているとき, 群コホモロジー を以下で定める.

$$H^n(G, M) := \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

命題 69. 群 G が加法群 M へ作用しているとき, 以下の自然な同型が得られる.

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \cong M^G,\ f \mapsto f(1).$$

注意 70. 上の命題より, 群コホモロジーは, 不変部分を取る, という関手の導来関手であることが分かる. とくに群 G が作用している加法群 M_1, M_2, M_3 の完全列 $0 \to M_1 \to M_2 \to M_3 \to 0$ (準同型は $\mathbb{Z}[G]$-加群としての準同型) に対して, 長完全列

$$0 \to M_1^G \to M_2^G \to M_3^G \to H^1(G, M_1) \to H^1(G, M_2) \to H^1(G, M_3) \to \cdots$$

が得られる.

補題 71. G が有限巡回群 $\langle\gamma\rangle \cong \mathbb{Z}/n\mathbb{Z}$ のとき

$$H^1(G, M) \cong \operatorname{Ker} t_G / \operatorname{Im}(1-\gamma).$$

ここで

$$t_G \colon M \to M,\ m \mapsto \sum_{g\in G} gm = \sum_{i=0}^{n-1} \gamma^i m,$$
$$1-\gamma \colon M \to M,\ m \mapsto m - \gamma m$$

とおいた.

略解. 一般の M の入射的分解を実際に書くのは難しい. 一方で $\mathbb{Z}[G]$-加群 $\mathbb{Z}$ は自然な射影的分解を持つ. 特に, 仮定のように, G が有限巡回群であれば

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}[G] \xleftarrow{f} \mathbb{Z}[G] \xleftarrow{g} \mathbb{Z}[G] \xleftarrow{f} \mathbb{Z}[G] \xleftarrow{g} \cdots$$

が射影的分解を与える. ただし

$$\epsilon \colon \mathbb{Z}[G] \to \mathbb{Z},\ \sum_{g\in g} n_g g \mapsto \sum_{g\in g} n_g,$$
$$f \colon \mathbb{Z}[G] \to \mathbb{Z}[G],\ \sum_{g\in g} n_g g \mapsto (1-\gamma)\sum_{g\in g} n_g g,$$
$$g \colon \mathbb{Z}[G] \to \mathbb{Z}[G],\ \sum_{g\in g} n_g g \mapsto \left(\sum_{g\in G} g\right)\left(\sum_{g\in g} n_g g\right)$$

である. 注意 66 で紹介したように, この射影的分解を用いて $H^n(G,M) = \operatorname{Ext}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ を明示的に計算することができる. □

問題 24. (1) $G = \{\pm 1\}$ (演算は掛け算), $M = \mathbb{R}$ とおき, 作用を

$$\{\pm 1\} \times \mathbb{R} \to \mathbb{R},\ (a, x) \mapsto ax$$

で定める. 上の補題を使って $H^1(\{\pm 1\}, \mathbb{R})$ を計算してみよ.

(2) $M = \mathbb{Z}$ として同様の作用を考え, $H^1(\{\pm 1\}, \mathbb{Z})$ を計算せよ.

略解. (1) $t_G \colon \mathbb{R} \to \mathbb{R}, x \mapsto x - x = 0$ だから $\operatorname{Ker} t_G = \mathbb{R}$. G の生成元は $\gamma = -1$ に注意して $1-\gamma \colon \mathbb{R} \to \mathbb{R}, x \mapsto x + x = 2x$. よって $\operatorname{Im}(1-\gamma) = \mathbb{R}$. すなわち $H^1(\{\pm 1\}, \mathbb{R}) \cong \mathbb{R}/\mathbb{R} = 0$ (零元のみからなる加群).

(2) 同様に $\operatorname{Ker} t_G = \mathbb{Z}$, $\operatorname{Im}(1-\gamma) = 2\mathbb{Z}$ が分かる. よって $H^1(\{\pm 1\}, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. □

Hilbert の定理 90

定理 72 (Hilbert 90)**.** L/K をガロア拡大とし, そのガロア群を $G := \mathrm{Gal}(L/K)$ とおく. 各元 $\sigma \in G$ は体の同型写像 $\sigma\colon L \to L$ だから, とくに乗法群 $L^\times := L - \{0\}$ へ制限すると, 群準同型 $\sigma\colon L^\times \to L^\times$ となり, 作用

$$G \times L^\times \to L^\times,\ (\sigma, x) \mapsto \sigma(x)$$

を得る. ($L^\times$ の演算は掛け算であるが, 可換群であるので, 加法群とみなせる.) このとき

$$H^1(G, L^\times) = 0 \text{ (零元のみからなる加群)}$$

となる.

応用. ピタゴラス数

定理 73. ピタゴラス数 x, y, z ($x^2 + y^2 = z^2$ 満たす自然数) は

$$x = t(m^2 - n^2),\ y = 2tmn,\ z = t(m^2 + n^2)\ (t, m, n \in \mathbb{N},\ m > n)$$

の形, または, x, y を入れ替えた形に書ける.

証明. $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ はガロア拡大で, $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) = \langle \rho \rangle$ (複素共役写像 ρ で生成される位数 2 の巡回群) となる. よって

$$H^1(G, \mathbb{Q}(\sqrt{-1})^\times) \cong \mathrm{Ker}\, t_G / \mathrm{Im}\,(1 - \gamma).$$

ここで $\mathbb{Q}(\sqrt{-1})^\times$ の演算は掛け算であることに注意して

$$\begin{aligned}
\mathrm{Ker}\, t_G &= \{\alpha \in \mathbb{Q}(\sqrt{-1})^\times \mid \alpha\rho(\alpha) = 1\} \\
&= \{x + y\sqrt{-1} \mid x, y \in \mathbb{Q},\ x^2 + y^2 = 1\}, \\
\mathrm{Im}\,(1 - \gamma) &= \left\{ \frac{\alpha}{\rho(\alpha)} \mid \alpha \in \mathbb{Q}(\sqrt{-1})^\times \right\} \\
&= \left\{ \frac{\frac{m + n\sqrt{-1}}{d}}{\frac{m - n\sqrt{-1}}{d}} = \frac{m^2 - n^2}{m^2 + n^2} + \frac{2mn}{m^2 + n^2}\sqrt{-1} \mid m, n, d \in \mathbb{Z}, (m, n) \neq (0, 0) \right\}
\end{aligned}$$

と計算できる. Hilbert 90 より

$$\mathrm{Ker}\, t_G = \mathrm{Im}\,(1 - \gamma),$$

とくに $\forall \alpha \in \mathrm{Ker}\, t_G,\ \exists \beta \in \mathrm{Im}\,(1 - \gamma)$ s.t. $\alpha = \beta$ である. すなわち

$$\begin{aligned}
&x, y \in \mathbb{Q},\ x^2 + y^2 = 1 \\
&\Rightarrow \exists m, n \in \mathbb{Z},\ (m, n) \neq (0, 0) \text{ s.t. } x = \frac{m^2 - n^2}{m^2 + n^2}, y = \frac{2mn}{m^2 + n^2}
\end{aligned}$$

を得る. すなわち

$$x^2+y^2=1 \text{ の有理数解は } x=\frac{m^2-n^2}{m^2+n^2}, y=\frac{2mn}{m^2+n^2} \text{ の形}$$

であることが分かった. この分母を払って題意を得る. □

注意 74. 証明は, 図を用いた初等的別解あり.

15　期末試験

去年度のもの

問題 1.　(1) 作用

$$M_2(\mathbb{Z}) \times \mathbb{Z}^2 \to \mathbb{Z}^2, \qquad \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} x \\ y \end{bmatrix} \right) \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$$

を考えたとき, $\mathbb{Z}^2$ は左 $M_2(\mathbb{Z})$-加群であることを示せ.

(2) 自由加群の定義を説明せよ.

(3) $\mathbb{Z}$-加群 $\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$ のねじれ元を全て求めよ.

問題 2.　(1) R を PID (単項イデアル整域) とする. 行列 $A \in M_{m\times n}(R)$ の単因子の定義を説明せよ.

(2) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \in M_{m\times n}(\mathbb{Z})$ の単因子を求めよ.

問題 3. $\mathbb{C}[T]$ を複素数係数の 1 変数多項式環とし, $f(T) \in \mathbb{C}[T]$ を生成元とする単項イデアルを $(f(T)) := f(T)\mathbb{C}[T]$ で表す.

(1) 複素ベクトル空間 $V := \mathbb{C}[T]/(T^2)$ を考える. 線形写像

$$\phi\colon V \to V, \quad p(T) \bmod (T^2) \mapsto Tp(T) \bmod (T^2)$$

の, 基底 $\{T \bmod (T^2), 1 \bmod (T^2)\}$ に関する表現行列を求めよ.

(2) 複素ベクトル空間 $V := \mathbb{C}[T]/(T^3 - 1)$ を考える. 線形写像

$$\psi\colon V \to V, \quad p(T) \bmod (T^3-1) \mapsto Tp(T) \bmod (T^3-1)$$

のジョルダン標準形を求めよ.

問題 4. R を環とし, N, M_1, M_2, M_3 を左 R-加群, $f\colon M_1 \to M_2$, $g\colon M_2 \to M_3$ を R-準同型写像とする. このとき $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ が完全列であれば

$$\mathrm{Hom}_R(N, M_1) \xrightarrow{f_*} \mathrm{Hom}_R(N, M_2) \xrightarrow{g_*} \mathrm{Hom}_R(N, M_3)$$

も完全列であることを示せ (f_* の単射性は示さなくてよい).

問題 5. 「自由加群は平坦加群である」が正しいかどうか答えよ. またその理由を説明せよ.

問題 6. R を環とし, M を左 R-加群とする. M がネター加群であれば, 任意の部分加群 $N \subset M$ もネター加群になることを示せ.

(配点: 1-(1), 1-(2), 1-(3), 2-(1), 2-(2), 3-(1), 3-(2), 4, 5, 6 各 10 点.)