代数学 B・演習　おぼえ書き　その 2

内容の誤りやタイプミスなど発見されましたら、横山までご一報下されば幸いです。
Contact: 4 号館 4103 院生室（1F セミナー室 3）／ yokoemon@gmail.com

今日の演習内容（＝前回の講義内容）

- **加群（module）と準同型**

  右 R-加群／左 R-加群の定義、R-部分加群、生成系と有限生成、商加群、R-準同型、準同型定理、核（kernel）と余像（coimage）・像（image）と余核（cokernel）

  定義はしっかりおさえておきましょう。色々な具体例を通して、加群とはどんなものなのかイメージがつかめると良いですね。

- **双対加群（dual module）**

  双対 R-加群の定義

  双対加群は後半で勉強するテンソル代数でもたくさん使います。これも重要。

前回の補足

- **演習問題 1-1：**一部誤解を招いていたようなので、ここで説明しておきます。

  まず演習中で服部先生が説明した内容ですが、これは大丈夫だと思います。行列

$$A = \begin{pmatrix} 1 & 2 & 3 & 2 & 1 \\ 3 & 6 & 9 & 6 & 3 \\ 1 & 2 & 4 & 1 & 2 \\ 2 & 4 & 9 & 1 & 5 \end{pmatrix}$$

  を列ベクトル $v = {}^t(x_1\ x_2\ x_3\ x_4\ x_5) \in \mathbb{R}^5$ に作用させて

$$Av = \begin{pmatrix} 1 \\ 3 \\ 1 \\ 2 \end{pmatrix} x_1 + \begin{pmatrix} 2 \\ 6 \\ 2 \\ 4 \end{pmatrix} x_2 + \begin{pmatrix} 3 \\ 9 \\ 4 \\ 9 \end{pmatrix} x_3 + \begin{pmatrix} 2 \\ 6 \\ 1 \\ 1 \end{pmatrix} x_4 + \begin{pmatrix} 1 \\ 3 \\ 2 \\ 5 \end{pmatrix} x_5$$

  を得ます。この中で線形独立な列ベクトルを探すために A の**列基本変形**を計算しました。一方、核の基底を求めるには $Av = 0$ を解けばよく、これは連立方程式

$$\begin{cases} x_1 & +2x_2 & +3x_3 & +2x_4 & +x_5 & = 0 \\ 3x_1 & +6x_2 & +9x_3 & +6x_4 & +3x_5 & = 0 \\ x_1 & +2x_2 & +4x_3 & +x_4 & +2x_5 & = 0 \\ 2x_1 & +4x_2 & +9x_3 & +x_4 & +5x_5 & = 0 \end{cases}$$

  を解くことと同じなので、A の**行基本変形**によって求められる、ということでした。

さて、基底を求めるだけなら**行基本変形だけでいいのでは？**という質問が出ていましたが、これは **正しい** です。行基本変形によって A は

$$\begin{pmatrix} 1 & 2 & 3 & 2 & 1 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

という階段型（echelon form）の行列に変形出来て、これより 1 列目と 3 列目**に対応するもとの列ベクトル**を像の基底としてとればよい、ということになるので、像の基底は

$$\left\{ \begin{pmatrix} 1 \\ 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 9 \\ 4 \\ 9 \end{pmatrix} \right\}$$

がとれることになります。

ここで、行基本変形をやってしまうと**像が動いてしまう**ことに十分注意して下さい。つまり

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\}$$

は像の基底**ではありません！**線形独立性が座標変換で不変であることから上のような求め方を使うことが出来るのですが、気を抜くと間違えてしまう可能性があります。服部先生が「間違えやすいので注意！」というアナウンスをしたのはこういう事情からでした。

- **演習問題 1-4(ii)：**普通に計算すると答えは $\displaystyle\prod_{0 \leq i \leq n-1} (p^n - p^i)$ ですが、n 個の基底の順序違いを考慮すればこれを $n!$ で割ったものが答えになります。
- **演習問題 1-7：**体の標数（characteristic）とは $n \cdot 1 = 1 + 1 + \cdots + 1 = 0$ をみたす最小の自然数 n のこと（存在しない場合は 0 で定義）。例えば $\mathrm{char}(\mathbb{F}_p) = p$（$p$ は素数）、$\mathrm{char}(\mathbb{Q}) = 0$ など。ちなみに体の標数は素数 p もしくは 0 の何れか。代数学 C でも詳しくやります。

チェックポイント

- **演習問題 2-2：群環**について少し復習しておきましょう。

  定義　R を可換環、G を群とする。このとき G 上の自由 R-加群[1] $R\langle G\rangle$ は次の積で環をなす。但し $r_g, r_{g'}, r_h, r_{h'} \in R$ とする。

  $$\left(\sum_{g \in G} r_g g\right)\left(\sum_{g' \in G} r'_{g'} g'\right) := \sum_{g, g' \in G} r_g r'_{g'} g g' = \sum_{g \in G} \left(\sum_{hh' = g} r_h r'_{h'}\right) g$$

  これを R 上の G の**群環（group ring）**といい、$R[G]$ で表す。

上で可換環 R を体 k に置き換えたもの（従って自由 R-加群が k-ベクトル空間に変わる）がテキスト p.73 に載っています。

また重要な性質として、G が可換であることと $R[G]$ が可換であることが必要十分です。

[1]定義はテキスト p.11。詳しくは次回の資料で紹介します。

- **演習問題 2-5,2-6,2-7：有限生成**に関するいくつかの性質

  以下 X を R-加群とし、M, N は X の R-部分加群とする。

  - M が有限生成で $f\colon\ M \to N$ が全射準同型ならば N も有限生成
  - M が有限生成ならば、その商加群 M/N も有限生成

  ただし

  - M が有限生成であっても、その R-部分加群 N は有限生成**とは限らない！**
    例えば可算無限個の変数をもつ $\mathbb{C}$ 係数多項式環 $\mathbb{C}[X_1, X_2, \cdots]$ を考えてみると、これは有限生成 $\mathbb{C}[X_1, X_2, \cdots]$-加群（$\{1\}$ で生成される）。しかしその $\mathbb{C}[X_1, X_2, \cdots]$-部分加群としてイデアル $(X_1, X_2, \cdots)$ を考えると、これは有限生成ではありませんね。ちなみに上の記号で R が Noether 環（Noetherian ring）と呼ばれる環の場合は、R-部分加群 N も有限生成となります。Noether 環の定義は少々わかりにくいかもしれませんが（例えばテキスト p.98 を参照）、これは R の任意のイデアルが有限生成であることと同値です。

- **演習問題 2-10：**この問題では左 $\mathrm{M}_n(\mathbb{Q})$-加群を考えるということで、R が非可換な例が登場しています。混乱している人がいるようなので少しだけ補足：

  まず、$\mathrm{Hom}_R(M, N)$ は（アーベル群として）いつでも定義可能です（つまり R は非可換でも OK）。しかし、ここに R-加群の構造を入れようとすると、R が非可換の場合は少々話がややこしくなります。今野先生が前回の講義の最後で「R は可換としましょう」と（例を交えて）説明されていましたが、おそらくこういった複雑な事情があったからだと思います。

  さて、**両側** (R, S)**-加群**（左 R 右 S-加群）の定義をしておきましょう。

  > **定義**　加法群 M が**両側** (R, S)**-加群**とは、M が左 R-加群かつ右 S-加群であって、両者の作用が可換（即ち $r \in R,\ s \in S,\ m \in M,\ (r \cdot m) \cdot s = r \cdot (m \cdot s)$ をみたす）。

  ここで、M を左（resp. 右）R-加群、N を両側 R-加群（つまり両側 (R, R)-加群）とすると、$\mathrm{Hom}_R(M, N)$ には自然に右（resp. 左）R-加群の構造が入ります。特に $N = R$ とすれば N はいつでも両側 R-加群ですから、M が左（resp. 右）R-加群ならば $M^* := \mathrm{Hom}_R(M, R)$ は自然に右（resp. 左）R-加群となります。これを**双対** R**-加群**[2]（dual R-module）と呼んだのでした。

  このように加群の構造に注意すれば、R が非可換な場合でも双対加群を考えることが出来ます。

- **準同型定理**　R-hom. $f\colon\ M \to N$ に対し $\mathrm{Coim}(f)$ と $\mathrm{Im}(f)$ が同型。

[2]加群の左右が入れ替わることが「双対」という名の由来です。

いろいろな例を知ろう

いろいろな加群（講義で出てきたもの以外で）：

- 任意の加法群 M は（自然な整数倍で）$\mathbb{Z}$-加群。
- $n \in \mathbb{N}$ に対し、R^n は成分ごとの演算で左 R-加群。これを階数 n の自由 R-加群（free R-module of rank n）という。
- R-係数多項式環 $R[X]$ や行列環 $\mathrm{Mat}_n(R)$ は自然に R-加群。
- (m,n) 型行列全体 $\mathrm{Mat}_{(m,n)}(R)$ は通常のスカラ倍で左 R-加群。またこのとき左 R-加群として $\mathrm{Mat}_{(m,n)}(R) \simeq R^{mn}$。
- 環 $R = (R,+,\cdot,0,1)$ の元 x,y に対し[3]、$x \star y := y \cdot x$ で演算 $\star$ を定めると、$R^{\mathrm{op}} := (R,+,\star,0,1)$ は環をなす。これを R の**逆環**または**反対環（opposite ring）**という。このとき

$$\text{右 } R\text{-加群 } M = (M,+,\cdot,0) \quad \Longleftrightarrow \quad \text{左 } R^{\mathrm{op}}\text{-加群 } M = (M,+,\star,0)$$

  注意：R が可換環ならば $R \simeq R^{\mathrm{op}}$ ですね。

その他の例は追って紹介します。続いて単純加群（simple module）の例：

- $\mathbb{C}^n$ は左 $\mathrm{Mat}_n(\mathbb{C})$-単純加群。
- 加法を演算とするアーベル群 G を $\mathbb{Z}$-加群とみると、G が $\mathbb{Z}$-単純加群となるには $\#G = p$（p は素数）となることが必要十分。
- $R = F$（体）の場合は、R-単純加群とは 1 次元 F-ベクトル空間のこと。

他にも（有名どころでは）こんな加群が活躍しています：

- ムーンシャイン加群（Moonshine module）V^{MS}：頂点作用素代数（VOA:Vertex Operator Algebra）の最も重要な例であり、$\mathbb{M} := \mathrm{Aut}(V^{\mathrm{MS}})$ は有名なモンスター単純群と呼ばれています。これは 26 個の散在型有限単純群のうち位数最大のもので、その位数は

$$\begin{aligned}\#\mathbb{M} &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000\end{aligned}$$

  という巨大な数になります。すごいですね。

- D-加群（D-module）：線形微分方程式系を微分作用素環の上の加群とみなしたもので、佐藤-テイト予想（2008 年に R.Taylor らによって解決）などで有名な佐藤幹夫氏が創設し、現在では特異点論や表現論など様々な応用がなされています。
- 他には、コーエン・マコーレー加群（Cohen-Macaulay module）、テイト加群（Tate module）、岩澤加群（Iwasawa module）、ヒルベルト C^*-加群（Hilbert C^*-module） etc.

[3] 環 R の表記について：右から「環」「加法演算」「乗法演算」「零元」「積の単位元」。

小噺

最後にちょっとブレイク。ここ数回の講義・演習で「加群」や「Hom」という言葉をたくさん聞いたと思いますが、**これらを考えることの ありがたみ** について、少し考えてみましょう。

先学期に皆さんは「幾何学 A」でホモロジー論を勉強しましたよね[4]。このホモロジー群の計算では $\mathbb{Z}$-加群が必要不可欠でした。あまり意識してなかったなぁという方、実は知らないうちに加群を勉強していたんですね。
ちょっと背伸びした話をしますと、これは「トポロジー」と呼ばれる分野の話で、ここで出てくるホモロジーというのは **幾何的対象**から**代数的対象**を作るための手段 とみなすことができます。圏論（category theory）的な表現をすれば、多様体（manifold）の圏から加群の圏への関手（functor）になっています（圏論について詳しい事を知りたい人は下の「参考文献」を参照)。これにより、幾何的対象を代数的対象に移して色々な計算が出来るようになります。つまり「輪っか」という幾何的対象を「種数 1」という（計算可能な）代数的対象に変えることで見通しが良くなる、ということですね。こういった事は例えばコンピュータに問題を解かせるといった場面で大きな役割を果たしています。

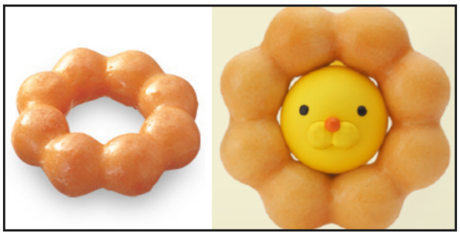

図 1：位相同型でない例（左は種数 1 ／右は種数 8）
よく見ると（顔の下も含め）8 つ穴がありますね

加えて、これらの代数的対象が**「位相不変」**であれば、これを観察するだけで 2 つの幾何的対象が位相同型でないことが判定出来るなど、メリットはたくさんあります。例えばある幾何的対象（例えば位相多様体）に対してそのホモロジー群やその rank（Betti 数)、Euler 数などは位相不変な量としてよく知られていますが、幾何学 A で勉強した「2 次元閉曲面の分類」にはそのホモロジー群 $\mathbb{Z}^{\oplus n}$ の n がいくつなのかをチェックすれば良かったわけです。こんな所で代数は（縁の下の力持ちとして）活躍していたんですね☆

[参考文献]　圏論について興味を持った方へ：

1. S. マックレーン「圏論の基礎」(シュプリンガー東京, 2005)
2. M.A.Arbib, E.G.Manes「Arrows, structures, and functors」(Academic Press, 1975)
   有名なのは日本語の [1]（原著は英語）ですが、私的には [2] がとても読みやすかったような記憶があります。本格的なものじゃなく大筋を知りたいという方には次がオススメです。
3. 谷村省吾「理工系のための トポロジー・圏論・微分幾何」(サイエンス社：別冊数理科学, 2006)

[4] 編入生の皆さんに補足：九大数理では学部 2 年の講義で「ホモロジー論」が必修になっています。位相空間論の復習から始まり、単体分割やチェインの定義を一通り身につけた後、ホモロジー群やバウンダリー作用素の計算方法を習得します。更に、完全列の概念とその応用（マイヤー・ヴィートリス完全系列など）を勉強します。