中山の補題のいろいろ
(環論入門：代数構造の非対称性を添えて)

March 30, 2025

自己紹介

1. 名前：朱里 (Twitter @akari0koutya)
2. 所属：徳島大学理工学部理工学科数理科学コース B1
3. 興味：スキーム論, 圏論, 可換環論, 表現論
4. spm29th 運営, すうがく徒のつどい運営
5. 数理の翼 42 夏季セミナー, 湧源

群論入門

群の定義

Definition 1.1
組 $(G, *)$ が次の条件を満たすとき群という：

1. 任意の $a, b, c \in G$ に対して, $a * (b * c) = (a * b) * c$ が成り立つ.
2. ある $e \in G$ が存在して, 任意の $a \in G$ に対して, $e * a = a * e = a$ が成り立つ.
3. 任意の $a \in G$ に対して, ある $b \in G$ が存在して, $a * b = b * a = e$ が成り立つ.

Definition 1.2
群 $(G, \cdot)$ が次の条件を満たすときアーベル群という：

1. 任意の $a, b \in G$ に対して, $a * b = b * a$ が成り立つ.

群の例

Example 1.3

1. 整数全体 $(\mathbb{Z}, +)$, 有理数全体 $(\mathbb{Q}, +)$, 実数全体 $(\mathbb{R}, +)$, 複素数全体 $(\mathbb{C}, +)$.
2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ から 0 を除いた乗法群 $(\mathbb{Q}\backslash\{0\}, \times)$,$(\mathbb{R}\backslash\{0\}, \times)$, $(\mathbb{C}\backslash\{0\}, \times)$.
3. $\mathbb{R}$, や $\mathbb{C}$ 上の n 次正方行列全体 $\mathrm{M}_n(\mathbb{R})$, $\mathrm{M}_n(\mathbb{C})$.

環論入門

(可換) 環論とは？

(可換) 環論とは主に (可換) 環を対象とする代数学の分野のこと.

では, 環とは？ $\to \mathbb{Z}$ や $\mathbb{Z}[\sqrt{-5}]$ に存在する豊かな構造を一般化したもの. 代数的整数論における素因数分解の一意性を考える文脈で Kummer が「理想数」を導入し, Dedekind がそれを整備することでイデアルが導入され, それに伴い環論が発展した. ring という言葉は ドイツ語の Ordnung (英：order) に由来する. (" おそらく "「秩序ある集合」という意味で, 「輪」を表すわけではない.)

環の定義

Definition 2.1
集合 R と二項演算 $+ : R \times R \to R$, $\times : R \times R \to R$ の組 $(R, +, \times)$ が次の条件を満たすとき環という :

1. $(R, +)$ は加法に関してアーベル群である.
   (i) 任意の $a, b, c \in R$ に対して, $a + (b + c) = (a + b) + c$ が成り立つ.
   (ii) 任意の $a \in R$ に対して, ある $-a \in R$ が存在して, $a + (-a) = 0$ が成り立つ.
   (iii) ある $0 \in R$ が存在して, 任意の $a \in R$ に対して, $a + 0 = a$ が成り立つ.
   (iv) 任意の $a, b \in R$ に対して, $a + b = b + a$ が成り立つ.
2. 任意の $a, b, c \in R$ に対して, $a(b + c) = ab + ac$ かつ $(a + b)c = ac + bc$ が成り立つ.
3. 任意の $a, b, c \in R$ に対して, $(ab)c = a(bc)$ が成り立つ.
4. ある $1 \in R$ が存在して, 任意の $a \in R$ に対して, $1a = a$ が成り立つ.

可換環の定義

Definition 2.2

環 R が次の条件を満たすとき可換環という：

1. 任意の $a, b \in R$ に対して, $ab = ba$ が成り立つ.

環の例

Example 2.3

1. 整数環 $\mathbb{Z}$, 有理数環 $\mathbb{Q}$, 実数環 $\mathbb{R}$, 複素数環 $\mathbb{C}$.
2. $\mathbb{R}$, や $\mathbb{C}$ 上の n 次正方行列全体 $\mathrm{M}_n(\mathbb{R})$, $\mathrm{M}_n(\mathbb{C})$.

準同型写像

Definition 2.4
環 R から環 S への写像 $f : R \to S$ が次の条件を満たすとき準同型という：

1. 任意の $a, b \in R$ に対して, $f(a+b) = f(a) + f(b)$ が成り立つ.
2. 任意の $a, b \in R$ に対して, $f(ab) = f(a)f(b)$ が成り立つ.
3. $f(1) = 1$ が成り立つ.

Remark 2.5
環の準同型写像は自然に加法の単位元を保つ：

$$f(0) = f(x - x) = f(x) - f(x) = 0.$$

環の準同型の例

Example 2.6

1. $\mathbb{Z}$ から $\mathbb{Z}/n\mathbb{Z}$ への自然な準同型写像 $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto [x]$.
2. $\mathbb{Z}$ から $\mathbb{Q}$ への自然な準同型写像 $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}, x \mapsto x/1$.
3. $\mathbb{C}$ から $\mathbb{C}$ への共役写像 $\bar{\cdot} : \mathbb{C} \to \mathbb{C}, x + y\sqrt{-1} \mapsto x - y\sqrt{-1}$.

Remark 2.7
環準同型写像は加法と乗法と単位元の構造を保つ写像, つまり, 環の構造を保つ写像である.

Definition 2.8 (自己準同型環)
R 加群 M の 自己準同型写像全体の集合を $\mathrm{End}_R(M)$ と書く. $\mathrm{End}_R(M)$ は (一般に可換とは限らない) 環となる.

環の準同型定理

Theorem 2.9
$f: R \to S$ を環の準同型写像とする. このとき, $R/\operatorname{Ker} f \cong \operatorname{Im} f$.

Example 2.10

1. 環準同型 $\phi : \mathbb{R}[x] \to \mathbb{C}, x \mapsto \sqrt{-1}$. このとき, $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

環上の加群

大学一年生のベクトル空間の振り返り

F を $\mathbb{R}$ または $\mathbb{C}$ とする. このとき, F 上のベクトル空間とは, 集合 V と
加法 $+ : V \times V \to V, (v, w) \mapsto v + w$ と
スカラー $\cdot : F \times V \to V, (a, v) \mapsto a \cdot v$ の組 $(V, +, \cdot)$ であって, 任意の
$u, v, w \in V, a, b \in F$ が次の条件を満たすもののことである：

1. $u + (v + w) = (u + v) + w.$
2. $u + v = v + u.$
3. V に 0 が存在して, 任意の $v \in V$ に対して, $v + 0 = v$ が成り立つ.
4. 任意の $v \in V$ に対して, ある $w \in V$ が存在して, $v + w = 0$ が成り立つ.
5. $a \cdot (v + w) = a \cdot v + a \cdot w.$
6. $(a + b) \cdot v = a \cdot v + b \cdot v.$
7. $a \cdot (b \cdot v) = (a \cdot b) \cdot v.$
8. $1 \cdot v = v.$

ベクトル空間の定義の修正版

このとき, F 上のベクトル空間とは, 集合 V と加法
$+ : V \times V \to V, (v, w) \mapsto v + w$ と
スカラー $\cdot : F \times V \to V, (a, v) \mapsto a \cdot v$ の組 $(V, +, \cdot)$ であって, 任意の
$u, v, w \in V, a, b \in F$ が次の条件を満たすもののことである :

1. 組 $(V, +)$ は加法に関してアーベル群である
2. $a \cdot (v + w) = a \cdot v + a \cdot w.$
3. $(a + b) \cdot v = a \cdot v + b \cdot v.$
4. $a \cdot (b \cdot v) = (a \cdot b) \cdot v.$
5. $1 \cdot v = v.$

環上の加群

Definition 3.1
環 R と加法 $+ : M \times M \to M$ とスカラー $\cdot : R \times M \to M$ の組 $(M, +, \cdot)$ が次の条件を満たすとき左 R 加群という :

1. $(M, +)$ は加法に関してアーベル群である.
2. 任意の $a \in R$ に対して, $a \cdot (v + w) = a \cdot v + a \cdot w$ が成り立つ.
3. 任意の $a, b \in R$ に対して, $(a + b) \cdot v = a \cdot v + b \cdot v$ が成り立つ.
4.
5. 任意の $a, b \in R$ に対して, $a \cdot (b \cdot v) = (a \cdot b) \cdot v$ が成り立つ.
6. 任意の $v \in M$ に対して, $1v = v$ が成り立つ.

Remark 3.2
スカラーの演算を $\cdot : M \times R \to M$ にしたものを 右 R 加群 という. また, R が可換なとき, 左 R 加群と右 R 加群は同じものである.

環上の加群を考える意義

Remark 3.3
環上の加群は, 環論の基本的な概念であり, 代数幾何学, 代数トポロジー, 表現論, 代数的整数論など代数のほとんどの分野で重要な役割を果たす. 次の代数と幾何の双対が考えられる :

1. 環 R は, ある空間上の関数の環と見なされるべきものである.
2. R 加群は, その空間上のベクトル束の切断の空間とみなすべきものである.

より噛み砕くと, 加群とは,「空間を測定・特徴づける追加の関数を提供するもの」と言える.

閑話休題：代数幾何学の基本的な概念

Definition 4.1

$$
\begin{aligned}
\operatorname{mSpec} R &:= \{\mathfrak{m} \subsetneq R \mid \mathfrak{m}\text{は}R\text{の極大イデアル}\} \\
\operatorname{Spec} R &:= \{\mathfrak{p} \subsetneq R \mid \mathfrak{p}\text{は}R\text{の素イデアル}\} \\
\mathrm{D}(I) &:= \{\mathfrak{p} \in \operatorname{Spec} R \mid I \not\subseteq \mathfrak{p}\} \\
\mathrm{V}(I) &:= \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} \\
\operatorname{rad}(R) &:= \bigcap_{\mathfrak{m} \in \operatorname{mSpec} R} \mathfrak{m} \\
\operatorname{nil}(R) &:= \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}.
\end{aligned}
$$

Remark 4.2
$\mathrm{D}(I)$ は開集合の公理を満たし, これによって $\operatorname{Spec} R$ に位相を入れることができる. この位相を *Zariski* 位相という.

Definition 4.3
局所環付き空間とは, 位相空間 X と, その上の環の層の組 $(X, \mathcal{O}_X)$ であって, 任意の $x \in X$ に対して, 茎 $\mathcal{O}_{X,x}$ が局所環であるもののこと.

局所環付き空間 $(X, \mathcal{O}_X)$ がアフィンスキームであるとは, ある環 A に対して, $(X, \mathcal{O}_X) \simeq (\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$ が成り立つことをいう.

Theorem 4.4
次の圏同値が成り立つ：

$$\mathrm{CRing}^{\mathrm{op}} \cong \mathrm{AffSch}$$

NAK

Lemma 5.1

R を環, I を R のイデアルとし, $I \subseteq \mathrm{rad}(R)$ を満たすとする. もし $r \in R$ が $a \equiv 0 \pmod{I}$ を満たすならば, $1 - r$ は R の単元である.

Proof.

$$(1-r)(1+r+\cdots+r^{n-1}) = 1 - r^n = 1$$

となるので, $1 - r$ は R の単元である. □

Theorem 5.2 (ケーリー・ハミルトンの定理)

環 R 上の n 次正方行列 A に対し, その固有多項式を $p_A(t)$ とする. このとき, $p_A(A) = 0$ が成り立つ.

Theorem 5.3 (一般化されたケーリー・ハミルトンの定理)

R 加群 M が R 上に n 個の元で生成され, $\phi \in \mathrm{End}_R(M)$, I が R のイデアルで $\phi(M) \subseteq IM$ ならば, M の写像として

$$\phi^n + r_{n-1}\phi^{n-1} + \cdots + r_1\phi + r_0 = 0, \quad r_i \in I^i (1 \leq i \leq n)$$

の関係が成り立つ.

Remark 5.4
$\phi : M_n(R) \to \mathrm{End}_R(R^n), e_j \mapsto \sum_{i=1}^n a_{ij}e_i$ で定められる環準同型写像は同型である. 上の定理の状況で, $M = R^n$ とすると, たしかに *Theorem 5.3* は *Theorem 5.2* の一般化となっている.

Theorem 5.5 (NAK,Krull-東屋の定理)

R を環, M を有限生成 R 加群, I を R のイデアルとし, $I \subseteq \mathrm{rad}(R)$ を満たすとする. もし $M = IM$ ならば, $rM = 0$, $r \equiv 1 \pmod{I}$ を満たす元 $r \in R$ が存在する. さらに, $I \subseteq \mathrm{rad}(R)$ ならば, $M = 0$ である.

Proof. Theorem 5.3 において, $\phi = \mathrm{id}_M$ とすると, $\phi(M) = M \subseteq IM$ なので,

$$r := 1 + r_1 + \cdots + r_n.$$

は M の写像として 0. したがって, $rM = 0$ であり, また, $r \equiv 1 \pmod{I}$ である. さらに, Lemma 5.1 より a は単元だから, $I \subseteq \mathrm{rad}(R)$ ならば, $M = 0$ である. □

Corollary 5.6

R を局所環, $\mathfrak{m}$ を R の唯一の極大イデアル, M を 有限生成 R 加群, $f_1, \ldots, f_n \in M$ を $\overline{f_1}, \ldots, \overline{f_n}$ が $M/\mathfrak{m}M$ の生成系となるような元とする. このとき, $f_1, \ldots, f_n$ は M の生成系である. 特に, $\mathfrak{m}/\mathfrak{m}^2$ の生成系は $\mathfrak{m}$ を生成する.

Proof. $N := (f_1, \ldots, f_n)$ を M の部分加群とする. このとき, $(N + \mathfrak{m}M)/\mathfrak{m}M = M/\mathfrak{m}M$ が成り立つ. 同型定理により $N + \mathfrak{m}M = M$ なので, $M/N = (N + \mathfrak{m}M)/N = \mathfrak{m}(M/N)$. これに, Theorem 5.5 を適用すると, $M/N = 0$ つまり $M = N$ が成り立つ. $\square$

圏論的な視点から

Definition 6.1
圏 $\mathcal{C}$ とは, 次のデータで構成される :

1. 対象の集まり $\mathrm{Ob}(\mathcal{C})$.
2. 任意の対象 $X, Y \in \mathrm{Ob}(\mathcal{C})$ に対して, X から Y への射の集まり $\mathrm{Hom}_{\mathcal{C}}(X, Y)$.

さらに, 以下の条件を満たす :

1. 任意の対象 $X \in \mathrm{Ob}(\mathcal{C})$ に対して, 恒等射 $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ が存在する.
2. 任意の対象 $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$ と射 $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ に対して, 射 $g \circ f \in \mathrm{Hom}_{\mathcal{C}}(X, Z)$ が存在する.
3. 任意の対象 $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$ と射 $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, $h \in \mathrm{Hom}_{\mathcal{C}}(Z, W)$ に対して, $(h \circ g) \circ f = h \circ (g \circ f)$ が成り立つ.

Example 6.2

1. Set : 集合を対象とし, 関数を射とする圏.
2. Grp : 群を対象とし, 準同型写像を射とする圏.
3. CRing : 可換環を対象とし, 環準同型写像を射とする圏.
4. Mod_R : 環 R 上の加群を対象とし, R 線型写像を射とする圏.
5. AffSch : アフィンスキームを対象とし, アフィンスキーム間の射を射とする圏.
6. Sch : スキームを対象とし, スキーム間の射を射とする圏.

Definition 6.3
$\mathcal{C}$ を圏とする. このとき, $\mathcal{C}$ の反対圏 $\mathcal{C}^{\mathrm{op}}$ とは, 次のデータで構成される :

1. 対象の集まり $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$.
2. 任意の対象 $X, Y \in \mathrm{Ob}(\mathcal{C})$ に対して, $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) := \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

Definition 6.4

1. $f : X \to Y$ がモノ射であるとは, 任意の $Z \in \mathrm{Ob}(\mathcal{C})$ と射 $g, h : Z \to X$ に対して, $f \circ g = f \circ h \Rightarrow g = h$ が成り立つことである.
2. $f : X \to Y$ がエピ射であるとは, 任意の $Z \in \mathrm{Ob}(\mathcal{C})$ と射 $g, h : Y \to Z$ に対して, $g \circ f = h \circ f \Rightarrow g = h$ が成り立つことである.

Example 6.5
集合の圏 Set において, モノ射は単射, エピ射は全射と同値. しかし, 一般の圏では, モノ射は単射, エピ射は全射とは限らない. 例えば, Ring ではエピ射と全射は一致しない.

Remark 6.6
圏 $\mathcal{C}$ と $\mathcal{C}^{\mathrm{op}}$ の関係を双対といい, $\mathcal{C}$ での主張はその射の向きを逆にした主張が $\mathcal{C}^{\mathrm{op}}$ での主張になる.

Example 6.7

1. モノ射とエピ射の定義は双対となっている.
2. 左 R 加群の圏 Mod_R は右 R^{op} 加群の圏 ${}_{R^{\mathrm{op}}}\mathrm{Mod}$ に圏同値の意味で等しい. (R^{op} は積の向きを逆にした環.)

応用と, 代数的構造の非対称性に関して

Theorem 7.1 (Vasconcelos)
R を環, M を有限生成 R 加群とする. R 線型写像 $f : M \to M$ が全射ならば同型である.

Remark 7.2
証明には, *Theorem* 5.5 を用いる.

Remark 7.3
R を環, M を有限生成 R 加群とする. R 線型写像 $f : M \to M$ が単射ならば同型である. これは真か？ $\to$ 答えは *No*.
(例えば, $R = \mathbb{Z}$, $M = \mathbb{Z} \oplus \mathbb{Z}$ とすると, $f : M \to M, (a, b) \mapsto (a, 0)$ は単射であるが同型ではない.)

Remark 7.4
この定理は Mod_R において, 単射と全射が双対でないことを表している. しかし, 体 k 上の有限次元ベクトル空間の圏 $(\mathrm{f.g.Vect})_k$ においては, 射が単射であることと全射であることは同値であった.

Theorem 7.5 (Vasconcelos)
有限生成 R 加群の任意の単射自己準同型写像が全射である必要十分条件は, R のすべての素イデアルが極大であること, である.

Example 7.6
$\phi_2 : \mathbb{Z} \to \mathbb{Z}, x \mapsto 2x$. これは単射だが全射でない例. 実際, $\mathbb{Z}$ は体でない *Dedekind* 整域なので, *Krull* 次元は 1 である.

Definition 7.7
R を環とする.

1. R 加群 M が *Hopfian* であるとは, M の任意の全射自己準同型写像が自己同型であることをいう.
2. R 加群 M が *co-Hopfian* であるとは, M の任意の単射自己準同型写像が自己同型であることをいう.

Theorem 7.8 (Ax-Grothendieck の定理)
S をスキーム, X を有限型 S スキームとする. このとき, X の *radiciel* な S 上の自己射は全射である.

Theorem 7.9 (特別な場合の Ax-Grothebendieck の定理)
多項式関数 $P:\mathbb{C}^n\to\mathbb{C}^n$ が単射ならば全単射である.

Remark 7.10
多項式関数 $P:\mathbb{C}^n\to\mathbb{C}^n$ が全射ならば全単射である. これは正しい ?
$\to$ 答えは *No.* 例えば, $P:\mathbb{C}\to\mathbb{C}, z\mapsto z^2$ は全射であるが単射ではない. ($\forall a\in\mathbb{C}$ に対し, $z^2=a$ を満たす $z\in\mathbb{C}$ が常に存在すれば良い. これは代数学の基本定理よりわかる.)

NAK の幾何学的解釈

Lemma 1 (幾何的 NAK)

X を *Noetherian* スキーム, $x \in X$ を閉点, U を x の開近傍, $\mathcal{F}$ を X 上の連接層とする. 切断 $a_1, \ldots, a_n \in \mathcal{F}(U)$ を 芽 $a_{1x}, \ldots, a_{nx} \in \mathcal{F}_x$ の像がファイバー $\mathcal{F}|_x := \mathcal{F}_x/\mathfrak{m}_x\mathcal{F}_x = \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} k(x) (= \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} (\mathcal{O}_{X,x}/\mathfrak{m}_x))$ を生成するものとする. このとき, あるアフィン開近傍 $\mathrm{Spec}(A) \ni x$ が存在し, $a_1|_{\mathrm{Spec}(A)}, \ldots, a_n|_{\mathrm{Spec}(A)}$ が $\mathcal{F}|_{\mathrm{Spec}(A)}$ を生成する.

1. 有限生成 R 加群 $\leftrightarrow \mathrm{Spec}(R)$ 上の連接層 $\mathcal{F}(\mathrm{Spec}(R))$ (X が locally Noetherian なので.)
2. x における切断の” 値 (芽)” がファイバーを張るなら, この切断は茎全体を生成する.

$\rightarrow$ Lemma 1 は連接層が閉点での振る舞いによって完全に決定されることを主張している.

- alg-d, 壱大整域, https://alg-d.com/math/kan_extension/.
- Grothendieck, A. , Éléments de géométrie algébrique IV.3, Étude locale des schémas et des morphismes de schémas, Troisième partie,Publications Mathématiques de l' IHÉS, 28 (1966), p. 5-255.
- 松村 英之, 復刊 可換環論 , 共立出版株式会社, 2009.
- Qing Liu, Algebraic geometry and arithmetic curves, 592 pp. Oxford Univ. Press 2002.
- Ravi Vakil' s Berkeley course notes https://virtualmath1.stanford.edu/~vakil/0708-216/
- Ulrich Görtz, Torsten Wedhorn, Algebraic geometry I. Schemes with examples and exercises, Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010. viii+615 pp.

Wolmer V. Vasconcelos, Injective Endomorphisms of Finitely Generated Modules, Source:Proceedings of the American Mathematical Society, Vol. 25, No. 4 (Aug., 1970), pp. 900-901.

Wolmer V. Vasconcelos, On finitely generated flat modules,Trans. Amer. Math. Soc. 138 (1969), 505-512. MR 39 #199.