可換代数の鳥瞰

mochix2

2020 年 6 月 7 日

まえがき

概要

可換代数の理論を紹介する.

可換代数とは, 可換環（以下単に環という）と呼ばれる対象を研究する数学の分野である. **環**とは, 大雑把に言えば加法と乗法の 2 つの演算が整合的に入っている集合のことで, 例えば整数全体 $\mathbb{Z}$ や, 複素係数 1 変数多項式全体 $\mathbb{C}[X]$ は自然に環の構造を持つ.

環を調べるために, 様々な道具を用いることができる. 例えば, 環が作用する可換群であるところの, **環上の加群**を調べることが効果的である. 加群の理論においては, 加群の準同型 $f, g\colon M \to N$ に対して常に $f+g$ を考えることができる, すなわち加群の圏に加法構造が自然にある, という点が環の理論と大きく異なっている. また, 環準同型 $f\colon A \to B$ に対し, B は自然に A 加群の構造を持つ（特に, A は自然に A 加群である）から, 加群を調べた結果が環に適用できることも多い. また環の**素イデアル**と呼ばれる特別な環の部分群を考えると, 素イデアルたちは環の情報を多く持っており, そこから多くの知識を引き出せることが分かってくる.

環の中でも, 特に性質の良いものがいくつかある. 例えば, 環であってイデアルの昇鎖条件を満たすものは, **ネーター環**と呼ばれる. 典型的な環はネーターなものが多く, また**剰余環**, **局所化**といった種々の構成に対しネーター性は保たれる. ネーター性を課すことは, 環にある意味で有限性を課すことであり, 環の構造は明瞭となり, 様々な理論がその上で展開できるようになる. また, 環であって極大イデアルがただ 1 つ存在するようなものは, **局所環**と呼ばれる. 局所環の構造は普通の環より調べやすいが, 重要なのは, 環についてのある主張を示す際に, 局所環の場合に帰着できることが多いという点にある.

本稿は, 代数を専攻していないが, 代数という分野の基本的なアイデアを概観したい人, あるいは代数を専攻していて整理された記述で復習したい人を対象に書いている（初めて代数に触れる人向けではない）.

内容

前提知識

基本的な集合論, 位相空間論, 圏論, 群論, 初等的な解析学の知識を仮定する. ただし, これらの非自明な結果を援用するときは, その旨を明記する. また, 初等的な代数学に触れたことがある, 数学科学部 3 年程度以上の読者を想定している.

記法

本稿では環はすべて単位的可換環であり, 環準同型は 1 を保つ. 加群の 1 倍写像は恒等写像である. 環準同型が定める代数が, 有限代数とは加群として有限生成であることであり, 有限型代数とはある有限変数多項式環からの全射な代数の準同型が存在することである. このことを, 環の射が有限である, 環の射が有限型であると呼ぶことにする. 体拡大が体として有限生成とは, 有限個の元の体としての付加によって得られることをいう.

$\mathrm{rad}(I)$ により I の根基, $\mathrm{jac}(I)$ により I の jacobson 根基を表す. ただし記号を乱用して $I = A$ のとき $\mathrm{rad}(A) = \mathrm{rad}(0)$, $\mathrm{jac}(A) = \mathrm{jac}(0)$ のことと約束する.

更新履歴

- 2019/12/26 執筆開始.
- 2020/06/07 1.1 執筆.

目次

1　可換環の基本

この章では, 環の定義とイデアルの定義からはじめ, 重要な環の構成とその初等的な性質について論じる. 素イデアルと極大イデアルの概念が導入されるが, これらは環について膨大な量の情報を含む. そのため対応原理を理解することは極めて重要である.

1.1　可換環とイデアル

定義 1.1.1. 集合 A とその上の二項演算 $+, \cdot$ の組が**環 (ring), 単位的可換環 (unital commutative ring)** であるとは, その加法 $+$ が 0 を単位元とする可換群の構造をもち, 乗法 $\cdot$ が 1 を単位元とする結合的可換単位的な演算であり, 加法と乗法が分配することをいう. すなわち, ある A の元 $0, 1$ が存在して任意の A の元 a, b, c に対し,

- $a + (b + c) = (a + b) + c$.
- $a + 0 = 0 + a = a$.
- $\exists x(a + x = x + a = 0)$.
- $a + b = b + a$.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- $a \cdot 1 = 1 \cdot a = a$.
- $a \cdot b = b \cdot a$.
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

をみたすことをいう. 上における加法逆元 x のことをふつう $-a$ と表し, また $a \cdot y = y \cdot a = 1$ を満たす元 y は (一般には存在しないが存在すれば) 乗法逆元と呼ばれ, a^{-1} と表される. 群論の初歩により, 単位元 $0, 1$ や加法逆元が一意的であること, 乗法逆元が存在すれば一意的であることがわかる.

文脈上明らかな場合は, 環 $(A, +, \cdot)$ のことを単に A と表す. また, $a \cdot b$ は ab と略記される.

注意 1.1.2. 簡単な計算により, $0x = 0$, $(-1)x = -x$ が成り立つ. また環の公理から, ” 常識的な演算” をすることができるとわかる. しかし, 環には乗法逆元が一般に存在しないから, 例えば $ab = cb$ に b^{-1} を乗じて $a = c$ とすることはできない.

一方で, 以下で説明する整域ならば, $ab = cb$ から $(a - c)b = 0$ と変形し, $b \neq 0$ ならば $a - c = 0$ すなわち $a = c$ を帰結することができる. 整域では逆元がなくても” 割り算ができる” という事実はよく用いられる.

定義 1.1.3. 環の元について,

環 A の元 a が**単元 (unit)** とは, $\exists b \in A(ab = 1)$ なること.

環 A の元 a が**零因子 (zero divisor)** とは, $\exists b \in A \setminus \{0\}(ab = 0)$ なること.

環 A の元 a が**冪零元 (nilpotent)** とは, $\exists n \in \mathbb{N}(a^n = 0)$ なること.

環 A の元 a が**冪等元 (idempotent)** とは, $a^2 = a$ なること.

環が**整域 (integral domain)** であるとは, $0 \neq 1$ であり, 零因子が 0 のみであることをいう.

環が**体 (field)** であるとは, $0 \neq 1$ であり, 0 以外の元が全て単元であることをいう.

単元全体の集合を $A^\times$ で表す. 零因子全体の集合を $Z(A)$ で表す.

注意 1.1.4. 整域の定義は, 単に $Z(A) = \{0\}$ と言い換えることもできる. 同様に, 体の定義は, 単に $A^\times = A \setminus \{0\}$ と言い換えることもできる. この場合, $1 \neq 0$ を課していることが見辛いのであえて上のように定義した.

命題 1.1.5. 単元, 零因子, 冪零元, 冪等元について以下が成り立つ.

- 冪零元は零因子である.
- 零因子は非単元である.
- 単元の積は単元. 逆に, 2 つの元の積が単元なら, もともと 2 つとも単元.
- 零因子と何かの積は零因子である. 逆に, 2 つの元の積が零因子なら, そのうち少なくとも 1 つは零因子.
- 単元と冪零元の和は単元である.
- 冪零元と冪零元の和は冪零元である.
- 冪等元 e に対し, $1-e$ も冪等元である.

Proof. 単元と冪零元の和について. 単元 u, 冪零元 x に対し $x^n = 0$ とする. $y = -x$ とおけば,

$$(u-y)(u^{n-1} + u^{n-2}y + \cdots + uy^{n-2} + y^{n-1}) = u^n - y^n = u^n$$

これは単元なので, よって $u + x = u - y$ も単元であることが従う.

冪零元と冪零元の和について. 冪零元 x, y に対し $x^n = 0$ かつ $y^m = 0$ ならば $(x+y)^{n+m-1} = 0$ が 2 項展開によりわかる.

それ以外の命題は定義からただちに従う. □

例 1.1.6. 整数全体からなる集合 $\mathbb{Z}$ は標準的な演算で環となる. これは整域だが体でない. 冪零元は 0 のみであり, 冪等元は $1, 0$ のみである. これを**有理整数環 (the ring of rational integers)** という.

有理数全体からなる集合 $\mathbb{Q}$, 実数全体からなる集合 $\mathbb{R}$, 複素数全体からなる集合 $\mathbb{C}$ は標準的な演算で環となる. これは整域であり, 体でもある. 冪零元は 0 のみであり, 冪等元は $1, 0$ のみである. これらは**有理数体, 実数体, 複素数体 (the field of rational numbers, real numbers, complex numbers)** と呼ばれる.

$\{0\}$ という集合に, ただ 1 通りの演算を入れることで環となる. これは**零環 (zero ring)** といい, 0 で表す. (すこし紛らわしい.) これは整域でも体でもない. $1 = 0$ が成り立っているからである. 冪等元は 0 のみ, 冪零元は 0 のみである. 逆に, $1 = 0$ が成り立つ環は, 任意の元 x に対し $x = 1x = 0x = 0$ が成り立つので, 零環であることがわかる.

注意 1.1.7. (零環は環か)

零環は非常に特殊な環であり, これを環の定義に入れてしまうことに疑問を持つ方もいるだろう. しかし, これは環の圏の終対象だったり, 全体イデアル (1) による剰余環だったり, 0 を含む積閉集合による局所化だったりする. つまり, 零環を環でないと定義すると, そのしわ寄せがいろんなところに来てしまい, 結果として理論が汚くなってしまう. (もっとも, Krull 次元など零環を除外して考えた方が自然な話も少なくない.) また, 整域や体に零環を許さないのは, 全体イデアル (1) は極大イデアルや素イデアルでないという定義に対応している. こちらも定義を別に変えてしまうと理論が汚くなるので, 本稿でしているような定義が現在一般的に用いられているのである.

大抵の場合, 零環に対する場合分けは簡単に済むので, ”例外的な環がある”という認識で問題ない.

定義 1.1.8. 環 A, B に対し, 写像 $f\colon A \to B$ が**環準同型 (ring homomorphism)** であるとは, 環構造を保つことをいう. すなわち, 任意の A の元 a, b に対し,

- $f(a+b) = f(a) + f(b)$.
- $f(ab) = f(a)f(b)$.
- $f(0) = 0$.
- $f(1) = 1$.

をみたすことをいう. 式の左辺にある $0, 1$ は A の元であり, 右辺にある $0, 1$ は B の元であることに注意.

群論の一般論により, 1 番目の条件から自動的に 3 番目の条件が出る. よって実は 3 番目の条件は不要である. 一方で, 4 番目の条件は必要であることが $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, n \mapsto (n, 0)$ なる例からわかる.

環準同型 $f\colon A \to B$ に対し, 環準同型 $g\colon B \to A$ が存在し, $f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$ が成り立つとき, f は**環同型 (ring isomorphism)** であるという.

簡単な計算により, 環準同型の合成は環準同型であること, 恒等写像は環準同型であることがわかる. (これにより可換環の圏 **CRing** が定まる.) また, 全単射環準同型は環同型となることもわかる.

命題 1.1.9. 有理整数環 $\mathbb{Z}$, 零環 0 は次の普遍性を持つ. すなわち, 任意の環 A に対して, $\mathbb{Z}$ から A への環準同型がただ 1 つ存在し, A から 0 への環準同型がただ 1 つ存在する. すなわち, $\mathbb{Z}, 0$ が CRing の始対象, 終対象であるということである.

この環準同型は, 明示的に表すとそれぞれ

$$f\colon \mathbb{Z} \to A, \begin{cases} n & \mapsto & f(n-1)+1 & (n>0) \\ 0 & \mapsto & 0 & \\ n & \mapsto & f(n+1)-1 & (n<0) \end{cases}$$

$$g\colon A \to 0, x \mapsto 0$$

となる.

注意 1.1.10. (有理整数環は何者か)

$\mathbb{Z}$ の演算や性質は, 中学高校で習った通りであるが, それが集合論的にどのように構成されたものか, ということは通常の数学科のカリキュラムでは習わないようである. 例えば, 今の定理では f を数学的帰納法のようなもので構成した, と見えるが, それが集合論的にはどう正当化されるかは, あまり知られていないようである. 現在の数学の主流である ZFC 公理系において, $\mathbb{Z}$ の構成, 写像の数学的帰納法による構成, などといった問題は, 集合論の初歩である順序数論の範疇に含まれる. この他, 数学をやる上で出くわす集合論的な問題については, 付録でまとめてある.

定義 1.1.11. 環 A に対し, その**イデアル (ideal)** とは加法とスカラー倍に閉じた A の空でない部分集合 I のことをいう. すなわち,

$$0 \in I \wedge \forall a, b \in I, r \in A (a+b \in I, ra \in I)$$

をみたすことをいう.

定義 1.1.12. 環 A をとる.

- 部分集合 $S \subseteq A$ に対し, S **の生成するイデアル (ideal generated by S)** $\langle S \rangle$ とは, S を含む最小の A

のイデアルのことである. これは常に存在し,

$$\{\sum_{i=0}^{n} a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N}\}$$

により与えられることがわかる. ただし, 0 個の和は 0 であると約束する.

- ただ 1 つの元により生成されるイデアル $\langle\{a\}\rangle$ のことを**単項イデアル, 主イデアル (principal ideal)** といい, (a) で表す. 特に, $(0) = \{0\}$ を**零イデアル (zero ideal)**, $(1) = A$ を**全体イデアル (unit ideal)** という. 全体イデアルでないイデアルのことを, **真のイデアル (proper ideal)** という. また, 全体イデアル, 零イデアルのことを合わせて**自明なイデアル**ということがよくある.
  明らかに, イデアルについて, 全体イデアルであること, 単元を含むこと, 1 を含むことは同値である.
- イデアルの族 $\{I_j\}_{j\in J}$ に対し, その**和**を, $\bigcup_{j\in J} I_j$ の生成するイデアルと定め, $\sum_{j\in J} I_j$ と書く. 有限族の和は $I_1 + \cdots + I_n$ とも書く. ただし, 0 個のイデアルの和は (0) と約束する.
- イデアルの族 $\{I_j\}_{j\in J}$ に対し, その**交叉**を, 集合論的交叉として定めるとイデアルになっていることがわかる. これを $\bigcap_{j\in J} I_j$ と書く. 有限族の交叉は $I_1 \cap \cdots \cap I_n$ とも書く. ただし, 0 個のイデアルの交叉は (1) と約束する.
- イデアルの有限族 $I_1, \ldots, I_n$ に対し, その**積**を, $\{\, x_1 \cdots x_n \mid x_j \in I_j \,\}$ の生成するイデアルと定め, $\prod_{j=1}^{n} I_j$ とか $I_1 \cdots I_n$ などと書く. ただし, 0 個のイデアルの積は (1) と約束する.
- イデアル I, J に対し, その**イデアル商 (ideal quotient)** を, $\{\, x \in A \mid \forall y \in J(xy \in I) \,\}$ として定めるとイデアルになっていることがわかる. これを $(I\colon J)$ と書く. 特に, 零イデアルとのイデアル商 $((0)\colon I)$ を I の**零化域, アナイアレータ (annihilator)** といい, $\mathrm{ann}_A(I)$ と書く.
- 一般に, 元 $a_1, \ldots, a_n$ があるときに, それが生成するイデアルのことを $(a_1, \ldots, a_n)$ とか $a_1A + \cdots + a_nA$ などと表す. この形で書けるイデアルは, **有限生成なイデアル (finitely generated ideal)** であるという. この記法はイデアルの和と整合的であることがわかる.

注意 1.1.13. イデアルの和, 積, 交叉は結合的単位的可換な演算であることが確かめられる. 有限生成イデアルの和, 積は再び有限生成となり, その生成元を書き下すことは難しくない. 一方で, 有限生成イデアルの交叉は一般に有限生成ではない.

誤解のおそれがないとき, 単項イデアル (x) のことを単に x と書くことがよくある. 例えば, $\mathrm{ann}((x)) = \mathrm{ann}(xA) = \mathrm{ann}(x)$ などと書く.

命題 1.1.14. イデアル I, J, K の和と積について次が成立する.

- $IJ \subseteq I \cap J \subseteq I \subseteq I + J$.
- $(I + J)K = IK + JK$.（積の分配）
- $I \subseteq K$ あるいは $J \subseteq K$ が成り立つと仮定する. このとき $(I + J) \cap K = (I \cap K) + (J \cap K)$.(交叉の分配)

また, イデアルの和は明示的に $I + J = \{\, a + b \mid a \in I, b \in J \,\}$ と書ける.

命題 1.1.15. イデアル商について次が成立する. ただし, 交叉と和は無限族についても成り立つ.

- $I \subseteq (I : J)$.
- $(I : J)J \subseteq I$.

- $((I:J):K)=(I:JK)=((I:K):J)$.
- $(\bigcap I_i:J)=\bigcap(I_i:J)$.
- $(I:\sum J_i)=\bigcap(I:J_i)$.

またアナイアレータに対しては, $Z(A)=\bigcup_{x\neq 0}\operatorname{ann}(x)$ が成立する.

定義 1.1.16. A,B を環, $f\colon A\to B$ を環準同型とする.

- A のイデアル I の**拡大 (extension)** とは, I の f による像 $f(I)$ の生成する B のイデアルのことをいう. これを I^e, IB などと書く.
- B のイデアル J の**縮約 (contraction)** とは, J の f による逆像 $f^{-1}(J)$ のことをいう. これは A のイデアルであることがわかる. これを J^c.$J\cap A$ などと書く. 特に, 零イデアルの縮約は f の**核 (kernel)** と呼ばれ, $\operatorname{Ker} f$ と書く.

後々わかるように, 拡大は A 加群 B のイデアル倍 IB と集合として一致する. また, A が B の部分環で f が包含写像のとき, 縮約は集合の演算 $J\cap A$ と集合として一致する. したがってこの記法は整合的である.

実際には, どの環準同型についての拡大縮約なのかというので混乱が生じやすいので, I^e, J^c という表記を使うことはまれである.

注意 1.1.17. f について単射であることと, 圏論的単射であることと, $\operatorname{Ker} f=(0)$ であることは同値である.

圏論的単射については, $\mathbb{Z}[x]$ からの射を考えればわかる.

命題 1.1.18. 拡大, 縮約について以下が成り立つ.

- 拡大, 縮約は包含を保つ.
- $I\subseteq I^{ec}, J^{ce}\subseteq J$.
- $I^e=I^{ece}, J^c=J^{cec}$.
- $I=I^{ec}$ であることは, $\exists J(I=J^c)$ であることに必要十分.
- $J=J^{ce}$ であることは, $\exists I(J=I^e)$ であることに必要十分.

以下の命題は, とてもよく使う.

命題 1.1.19. （拡大, 縮約と和, 積, 交叉の交換）

- $I^e+J^e=(I+J)^e$.
- $I^eJ^e=(IJ)^e$.
- $I^c\cap J^c=(I\cap J)^c$.

定義 1.1.20. 環 A の部分集合 S が**積閉集合, 乗法的集合 (multiplicatively closed set, multiplicative set)** とは, 1 を含み, かつ $\forall a,b\in S(ab\in S)$ をみたすことをいう.

例 1.1.21. A を環とする.

- $a\in A$ に対し, $\{1,a,a^2,\cdots\}$ は a で生成された積閉集合という.
- S を積閉集合とすれば, $\tilde{S}=\{x\in A\mid \exists y(xy\in S)\}$ も積閉集合である. これを S の飽和化という.
- 次の節で定義する素イデアル $\mathfrak{p}$ について, $A\setminus\mathfrak{p}$ は定義からただちに積閉集合である.

1.2　素イデアル

定義 1.2.1. A を環とする.

- A の真のイデアル $\mathfrak{p}$ が**素イデアル (prime ideal)** であるとは, 補集合 $A \setminus \mathfrak{p}$ が積閉集合をなすことをいう.
- A の真のイデアル $\mathfrak{m}$ が**極大イデアル (maximal ideal)** であるとは, 包含順序において真のイデアル全体の極大元であることをいう. すなわち, $\mathfrak{m} \subsetneq I$ を満たすイデアルは $I = (1)$ のみであることをいう.

1.3　剰余環

1.4　局所化

1.5　直積環

定義 1.5.1. 2 つのイデアル I, J が **comaximal** であるとは, $I + J = (1)$ であることをいう. より一般に, イデアルの族がどの相異なる 2 つのイデアルについても comaximal であるとき, **pairwise comaximal** という.

1.6　多項式環

1.7　一意分解整域

2 加群

2.1 加群

定義 2.1.1. 環 A に対し, 集合 M とその上の演算 $+\colon M\times M\to M$, $\cdot\colon A\times M\to M$ の組が A **加群 (A-module, module over A)** であるとは, その加法 $+$ が 0 を単位元とする可換群の構造をもち, スカラー乗法 $\cdot$ が環構造と両立するように M に作用することをいう. すなわち, ある M の元 0 が存在して任意の M の元 x,y,z, A の元 a,b に対し,

- $x+(y+z)=(x+y)+z$.
- $x+0=0+x=x$.
- $\exists w(x+w=w+x=0)$.
- $x+y=y+x$.
- $a\cdot(b\cdot x)=(ab)\cdot x$.
- $1\cdot x=x$.
- $(a+b)\cdot x=(a\cdot x)+(b\cdot x)$.
- $a\cdot(x+y)=(a\cdot x)+(a\cdot y)$.

をみたすことをいう. 上における加法逆元 w のことをふつう $-x$ と表す. 群論の初歩により, 単位元 0 や加法逆元が一意的であることがわかる.

文脈上明らかな場合は, A 加群 $(M,+,\cdot)$ のことを単に M と表す. また, $a\cdot x$ は ax と略記される.

簡単な計算により, $0x=0$, $(-1)x=-x$ が成り立つ.

定義 2.1.2. A 加群 M,N に対し, 写像 $f\colon M\to N$ が A **加群の準同型 (A-module homomorphism)** であるとは, 加群の構造を保つことをいう. すなわち, 任意の M の元 x,y, A の元 a に対し,

- $f(x+y)=f(x)+f(y)$.
- $f(0)=0$.
- $f(ax)=af(x)$.

をみたすことをいう. 環の場合と同様に, 2 番目の条件は実は不要である.

注意 2.1.3. $a\in A$ を固定し, $\lambda_a\colon M\to M, x\mapsto ax$ なる写像を考える. 加群の公理は, これが加群の準同型であり, しかも $\lambda_a+\lambda_b=\lambda_{a+b}, \lambda_a\circ\lambda_b=\lambda_{ab}$ であることを述べている. 非可換環の言葉を用いると, 可換群 M に A 加群の構造を入れることは A から M の自己群準同型のなす非可換環への非可換環準同型を定めるということに等しい.

定義 2.1.4. 環 A,B に対し, 集合 M とその上の演算 $+\colon M\times M\to M$, $\cdot_A\colon A\times M\to M$, $\cdot_B\colon B\times M\to M$ の組が (A,B) **複加群 ((A,B)-bimodule)** であるとは, $(M,+,\cdot_A)$ が A 加群であり, $(M,+,\cdot_B)$ が B 加群であり, さらに

$$\forall a\in A, b\in B, x\in M(a\cdot_A(b\cdot_B x)=b\cdot_B(a\cdot_A x))$$

をみたすことをいう.

2.2　部分加群と剰余加群

2.3　極限と余極限

2.4　完全性

例 **2.4.1.** [9] からの例.

$\mathbb{Q}[X]$ の部分環 R を, 定数項が整数, 1 次の項が 0, 2 次以上の項が有理数である多項式全体として定める. $I = X^2R, J = X^3R$ なる単項イデアルをとる. $I \cap J$ は 5 次未満の項が 0, 5 次以上の項が有理数である多項式全体のなすイデアルであることが計算で分かる. これが有限生成で, $f_1R + \cdots + f_nR$ と書けると仮定する.

$f_i = X^5 g_i$ として, g_i の定数項を既約分数 a_i/b_i で書く. $g = (b_1 \cdots b_n + 1)^{-1} X^5$ とすれば, $g \in I \cap J$ であるから $g = f_1 h_1 + \cdots + f_n h_n (h_i \in R)$ と書ける.

そこで両辺を X^5 で割ってから $X = 0$ を代入すれば, $(b_1 \cdots b_n + 1)^{-1} = (a_1/b_1)h_1(0) + \cdots (a_n/b_n)h_n(0)$ であり, $b_1 \cdots b_n$ を両辺に乗じると左辺は分数, 右辺は整数となり矛盾する. したがって, $I \cap J$ は有限生成でないことがわかった.

一方, 環 R が pseudo-coherent なら, 有限生成イデアル I, J に対し R 加群の短完全列

$$0 \longrightarrow I \cap J \longrightarrow I \oplus J \xrightarrow{f} I + J \longrightarrow 0$$

において $I + J$ が有限表示, $I \oplus J$ が有限生成だから $I \cap J$ は有限生成.

2.5　有限性

2.6　行列

2.7　テンソル積

2.8　局所化

2.9　平坦性

C　群論要約

群とは, 結合的単位的かつ全ての元が可逆な演算をもつ数学的対象のことである. 例えば X という対象ごとに, その自己同型全体 $\mathrm{Aut}(X)$ は自然に群の構造を持つから, 群の概念は数学の各所に現れ, 重要である. 特に有限群にはいくつか構造を調べる手段があり, それを利用することで X を調べることが出来ることがある (ガロア拡大の理論が典型的である).

我々はまず, 群と群準同型, 群作用について調べる. Lagrange の定理, Orbit-Stabilizer, 類等式を示すことで, 群の位数についての最も基本的な情報を得ることができる. 有限群論の基本的な定理である, Sylow の定理を示し, 群にはたくさんの部分群が, ある秩序の元で存在することを見る.

定義 C.0.1. (群)

集合 G とその上の 2 項演算 $\cdot\colon G\times G\to G$ の組が**群 (group)** であるとは, ある G の元 e があり, 任意の G の元 x,y,z に対し,

- $x\cdot(y\cdot z)=(x\cdot y)\cdot z$.
- $x\cdot e=e\cdot x=x$.
- $\exists w(x\cdot w=w\cdot x=e)$.

をみたすことをいう. さらに, 任意の G の元 x,y に対し,

- $x\cdot y=y\cdot x$.

をみたすとき, 特に **Abel 群 (abelian group)** という. Abel 群は一意的な $\mathbb{Z}$ の作用により $\mathbb{Z}$ 加群となることが確かめられるので, 加群の理論をそのまま適用できる.

定義の e は実は一意的であるとわかり, 群の単位元という. また各 $x\in G$ に対し定義の w も一意的であり, x の逆元という. 逆元は x^{-1} と表される.

群 G の元の個数 $|G|$ を, その群の**位数 (order)** という.

群 G,H の間の写像 $f\colon G\to H$ が**群準同型 (group homomorphism)** とは, 任意の $x,y\in G$ に対し,

- $f(x\cdot_G y)=f(x)\cdot_H f(y)$.
- $f(e_G)=e_H$.

をみたすことをいう. (実は 2 番目の条件は 1 番目の条件から出る.) ただし, 各群の演算や単位元を下付きの添字で表した.

群と群準同型により, 群の圏 Grp を得る. このとき, 群の圏の同型は全単射群準同型のことだとわかる.

群の演算は, たびたび省略される. また, $x\in G$ の n 回の積を x^n, x^{-1} の n 回の積を x^{-n}, 単位元を x^0 と表す. 指数法則 $x^{n+m}=x^nx^m$ が成り立つことは簡単な場合分けでわかる.

定義 C.0.2. (部分群)

群 G の部分集合 $H\subseteq G$ であって, 演算の制限で群となり, 包含写像が群準同型であるものを G の**部分群 (subgroup)** という. (演算の制限で群となるならば, 自動的に包含写像は群準同型になるとわかるので, 実は 2 番目の条件は不要である.)

部分群の代表的な例を挙げる.

- G, $\{\, e \,\}$ は自明な部分群である.
- 部分群の族が与えられたとき, その交叉は再び部分群となる.
- 群 G の部分集合 $S \subseteq G$ に対し, S を含む部分群すべての交叉を考えることで, 最小の G の部分群が存在する. これを S により**生成された群 (group generated by S)** といい, $\langle S \rangle$ で表す. 特に $x \in G$ により生成される部分群を $\langle x \rangle$ で表す. $\langle x \rangle$ の位数のことを, x の**位数**という. この値は, $x^n = e$ なる最小の正の整数 n に一致する.
- 群準同型 f に対し, 部分群の逆像は部分群である. 特に $\{\, e \,\}$ の逆像は f の**核 (kernel)** と呼ばれ, $\operatorname{Ker} f$ と表す. $f\colon G \to H$ が単射であることと, 圏論的単射であることと, $\operatorname{Ker} f = \{\, e_G \,\}$ であることは同値である.
- 群準同型 f に対し, 部分群の像は部分群である. 特に G の像は f の**像 (image)** と呼ばれ, $\operatorname{Im} f$ と表す. $f\colon G \to H$ が全射であることと, 圏論的全射, $\operatorname{Im} f = H$ であることは同値である.[*1]

定義 C.0.3. 群作用、準同型としてのみかた

定義 C.0.4. 軌道、軌道分解、剰余類、剰余類分解

定理 C.0.5. (Lagrange の定理) 群 G とその部分群 H に対し, $|G| = |H|\,|G/H|$ が成り立つ. 特に有限群において, 部分群の位数や元の位数は $|G|$ を割り切る.

Proof. □

定義 C.0.6. 固定化群, 中心化群中心、正規化群

定理 C.0.7. (Orbit-Stabilizer)

Proof. □

定理 C.0.8. (類等式)

Proof. □

定義 C.0.9. 正規部分群、剰余群

命題 C.0.10. 正規部分群の特徴

Proof. □

定理 C.0.11. (対応原理)

Proof. □

定理 C.0.12. (準同型定理 (第 1 同型定理), 第 2 同型定理, 第 3 同型定理)

Proof. □

[*1] https://ncatlab.org/toddtrimble/published/monomorphisms+in+the+category+of+groups

定義 C.0.13. p 群

定理 C.0.14. (Sylow の定理)

Proof. □

定義 C.0.15. 直積, 半直積

命題 C.0.16. 内部直積条件

Proof. □

命題 C.0.17. 内部半直積条件

Proof. □

ここで紹介した理論以外にも, 単純群と組成列の一意性 (Jordan-Hölder の定理) に関する理論, 冪零群, 可解群, 表現論の手法など様々な群についての理論がある. 有限群の完全な分類をするのは, 一般には非常に難しい.

典型的には可換な場合を先に解決し, 非可換な場合は Sylow 部分群が何個あるかなどを調べて場合分けしたり, うまく部分群をとって半直積の分類に帰着したりすることで行う. しかしこの方法は, 位数が小さいときや, 特別な素因数分解ができる場合などに限られがちである. そこで次善の策として有限単純群の完全な分類をすることが考えられるが, これはすでに完成している (ただし証明はとてつもなく長大とのことだ).

参考文献

[1] M.F.Atiyah and I.G. MacDonald,『Atiyah-MacDonald　可換代数入門』(新妻弘訳), 共立出版, 2006.
[2] 松村英之,『復刊　可換環論』, 共立出版, 2000.
[3] 雪江明彦,『代数学 2　環と体とガロア理論』, 日本評論社, 2010.
[4] 志甫淳,『層とホモロジー代数』, 共立出版, 2016.
[5] 藤崎源二郎,『体とガロア理論』, 岩波書店, 1991.
[6] 清水勇二,『現代基礎数学 16　圏と加群』, 朝倉書店, 2018.
[7] 斎藤毅,『大学数学の入門 7　線形代数の世界　抽象数学の入り口』, 東京大学出版会, 2007.
[8] 寺田至・原田耕一郎,『群論』, 岩波書店, 2006. https://math.berkeley.edu/ kpmann/SylowNotes.pdf
[9] https://math.stackexchange.com/questions/295875/intersection-of-finitely-generated-ideals
https://mathoverflow.net/questions/8324/what-does-linearly-disjoint-mean-for-abstract-field-extensions

文献紹介