抽象代数ポータル

19 pages

Table of Contents

data/lecture/math/abstract-algebra/抽象代数ポータル-講義.n.md md d645a9b

抽象代数 ポータル

abstract algebra

抽象代数 は、数そのものではなく、数や変換や対称性が持つ演算の 形 を調べる分野である。最初に大切なのは、群、環、体を名前だけで覚えないことである。これらは全て、「どの演算を許し、その演算で何が保存され、何が 失 われるか」を整理するための言語である。

抽象化の目的は、具体例を捨てることではない。具体例に 共通 する構造を取り出し、同じ議論を別の 対象 にも移せるようにすることである。

1 先に必要な見方

抽象代数 は、離散数学の上に立っている。特に次の内容を前提にする。

→ 講義 **命題・述語と量化** lecture math discrete-math

https://study.bem130.com/lecture/math/discrete-math/命題・述語と量化-講義/

→ 講義 **同値関係と分割** lecture math discrete-math

https://study.bem130.com/lecture/math/discrete-math/同値関係と分割-講義/

→ 講義 **商集合と自然な射影** lecture math discrete-math

https://study.bem130.com/lecture/math/discrete-math/商集合と自然な射影-講義/

→ 講義 **写像の基本** lecture math discrete-math

https://study.bem130.com/lecture/math/discrete-math/写像の基本-講義/

2 読む順番

最初に、演算と構造を見る。

→ 講義 **代数的構造とは何か** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/代数的構造とは何か-講義/

→ 講義 **二項演算と閉包性** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/二項演算と閉包性-講義/

次に、同じものとみなす操作を学ぶ。これは商群や商環の前提である。

→ 講義 **同値関係と剰余類の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/同値関係と剰余類の基本-講義/

→ 講義 **合同式と mod 演算の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-講義/

そのあと、群を学ぶ。

→ 講義 **半群・モノイド・群への入口** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/半群・モノイド・群への入口-講義/

→ 講義 **群の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/群の基本-講義/

→ 講義 **部分群と生成** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/部分群と生成-講義/

→ 講義 **剰余類とラグランジュの定理** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/剰余類とラグランジュの定理-講義/

→ 講義 **正規部分群と商群** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/正規部分群と商群-講義/

→ 講義 **群準同型と同型** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/群準同型と同型-講義/

→ 講義 **群作用と対称性** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/群作用と対称性-講義/

最後(さいご)に、二(ふた)つの演算(えんざん)を持(も)つ構造(こうぞう)である環(かん)と体(たい)へ進(すす)む。

→ 講義 **環の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/環の基本-講義/

→ 講義 **イデアルと商環** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/イデアルと商環-講義/

→ 講義 **整域・零因子・多項式環** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/整域・零因子・多項式環-講義/

→ 講義 **体の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/体の基本-講義/

→ 講義 **有限体の入口** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/有限体の入口-講義/

→ 講義 **準同型の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/準同型の基本-講義/

→ 講義 **準同型定理の見取り図** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/準同型定理の見取り図-講義/

3 何を変えて何を保存するか

見方	変えるもの	保存したいもの
同値関係	個々の代表元	同じ類に属するという分類
商構造	元を類へまとめる	演算が代表元によらないこと
準同型	対象の表示	演算の構造
同型	元の名前	全ての代数的関係
群作用	群を変換として見る	対称性の構造

この表は、抽象代数全体の読み方である。定義を見たら、必ず「何を変え、何を変えないための定義か」を確認する。

4 演習リンク

→ 基本演習 **代数的構造と二項演算** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/代数的構造と二項演算-基本演習/

→ 基本演習 **同値関係と合同式** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/同値関係と合同式-基本演習/

→ 基本演習 **群と部分群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/群と部分群-基本演習/

→ 基本演習 **剰余類・正規部分群・商群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/剰余類・正規部分群・商群-基本演習/

→ 基本演習 **準同型と同型** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/準同型と同型-基本演習/

→ 基本演習 **環・イデアル・商環** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/環・イデアル・商環-基本演習/

→ 基本演習 **整域・体・有限体** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/整域・体・有限体-基本演習/

5　まとめ

抽象代数 は、演算を持つ対象 を比較するための言語である。群は一つの演算、環は足し算と掛け算、体はさらに割り算ができる環を 扱 う。準同型と商構造を通して、具体的な計算と 抽象的 な構造がつながる。

data/lecture/math/abstract-algebra/代数的構造とは何か-講義.n.md md e34dbcb

代数的構造とは何か

algebraic structure

抽象代数 で最初に固定したい見方は、対象 を「集合 と演算の組」として見ることである。数の集合だけ を見ても、まだ代数は始まらない。その 集合 の中で、どの演算を 行 い、その演算がどの法則を満たすかを 指定して初めて、代数的構造になる。

たとえば整数全体 $\mathbb{Z}$ は、足し算と一緒に見ると群になる。しかし掛け算と一緒に見ると、0 以外の 元 全て に 逆元 があるわけではないので群にはならない。同じ集合でも、演算を変えると構造が変わる。

ここでの群と 逆元 は、あとで正式に定義する用語である。この段階では、「集合だけでなく演算も指定 しないと構造は決まらない」という点だけを使う。

1 定義の形

代数的構造は、典型的には

$$(S, *)$$

または

$$(S, +, \cdot)$$

の形で書く。ここで S は集合であり、$*$、$+$、$\cdot$ は演算である。

この表記は、「元 が何か」と「元 どうしをどう操作するか」を分けている。集合だけでは要素の一覧であ り、演算だけではどこで計算するかが分からない。両方 を指定して初めて、計算の世界が定まる。

2 何故公理で定義するのか

公理は、具体例の細部を忘れ、議論に必要な性質だけを残すための 条件 である。

整数の足し算、平面の回転、正方形の対称性は見た目がまったく違う。しかし、どれも「合成できる」「何もしない操作がある」「元 (element) へ戻す操作がある」という共通点を持つ。この共通点だけを取り出すと、群 (group) の公理になる。

→ 講義 **群の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/群の基本-講義/

3 何が変わり、何が保存されるか

抽象化では、具体的な表示は変わる。整数、行列、置換、剰余類は見た目が異なる。一方で、演算 (operation) の満たす法則は保存して見る。

たとえば、同型な二つの群 (group) は、元 (element) の名前は違っても、演算表の構造は同じである。つまり、どの元 (element) を組み合わせるとどの元 (element) になるかという情報が保存される。同型は後で準同型と一緒に定義するので、ここでは「名前が変わっても演算の対応が残る」という見通しとして読めばよい。

→ 講義 **群準同型と同型** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/群準同型と同型-講義/

4 具体例：同じ集合 (set) でも構造は変わる

集合 (set) $\mathbb{Z}$ を考える。

$$(\mathbb{Z}, +)$$

は群 (group) である。0 が単位元 (identity element) であり、整数 a の 逆元 (inverse element) は $-a$ である。

しかし

$$(\mathbb{Z}, \cdot)$$

は群 (group) ではない。たとえば 2 の 乗法逆元 は整数の中に存在しない。もし $2b = 1$ となる整数 b があれば、左辺は偶数なので 1 にはならない。

ここで大切なのは、集合 (set) だけを見て「群 (group) かどうか」を言えない点である。必ず演算 (operation) と組にして判断する。

5　他分野との接続

抽象代数は線型代数にも現れる。たとえば可逆行列全体は、行列積によって群 (group) をなす。

→ 講義 **逆行列の基本** lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/逆行列の基本-講義/

この節は接続の見通しであり、行列の知識を以後の定義や証明の前提にはしない。

整数論では、剰余類の足し算や掛け算が抽象代数の基本例になる。

→ 講義 **整数論ポータル** lecture math number-theory

https://study.bem130.com/lecture/math/number-theory/整数論ポータル-講義/

6　演習リンク

→ 基本演習 **代数的構造と二項演算** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/代数的構造と二項演算-基本演習/

7　まとめ

代数的構造 (algebraic structure) とは、集合 (set) と演算 (operation) を組にして、公理で必要な性質を指定したものである。同じ集合 (set) でも演算 (operation) が変われば構造は変わる。抽象代数では、見た目ではなく、演算 (operation) で保存される構造を見る。

data/lecture/math/abstract-algebra/二項演算と閉包性-講義.n.md md f0b87eb

二項演算と閉包性

binary operation　closure

抽象代数で最初に確認すべき操作は、二つの元から一つの元を作る操作である。これを二項演算という。

binary operation

集合 S 上の二項演算とは、写像

$$* : S \times S \to S$$

のことである。つまり、任意の $a, b \in S$ に対して、結果 $a * b$ が再び S の元になる。

ここでいう写像は、入力 に対して 出力 を一つ定める規則である。$S \times S$ は S の元を二つ並べた組の集合を表す。

この「結果が同じ集合の中に戻る」という条件が閉包性である。

1　何故閉包性が必要か

閉包性がないと、演算を繰り返せない。

たとえば自然数全体 $\mathbb{N}$ で引き算を考えると、

$$2 - 5 = -3$$

は自然数ではない。したがって引き算は $\mathbb{N}$ 上の二項演算ではない。

一方、整数全体 $\mathbb{Z}$ で引き算を考えると、任意の整数 a, b に対して $a - b$ は整数である。したがって引き算は $\mathbb{Z}$ 上の二項演算である。

2　結合法則と可換性

結合法則は、三つ以上の元を演算するときに括弧の位置が結果に影響しないことを表す。

associative law

$$(a * b) * c = a * (b * c)$$

結合法則があると、$a * b * c$ と書いても意味が曖昧にならない。

可換性は、順序を入れ替えても結果が変わらないことを表す。
commutativity

$$a * b = b * a$$

可換性は常に仮定されるわけではない。行列積や置換の合成は一般に可換でない。

→ 講義 **行列の積の意味** lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/行列の積の意味-講義/

行列と置換は非可換な演算の例として挙げているだけで、このページの判定には使わない。

3 単位元と逆元

単位元とは、演算しても相手を変えない元である。
identity element

$$e * a = a * e = a$$

逆元 とは、演算によって単位元へ戻す元である。
inverse element

$$a * a^{-1} = a^{-1} * a = e$$

単位元と逆元は、方程式を解くために重要である。もし $a * x = b$ を解きたいなら、左から a^{-1} を作用させて $x = a^{-1} * b$ としたくなる。この操作ができるためには、逆元が必要である。

4 具体例：演算表で見る

集合 $S = \{0, 1, 2\}$ に、3 で割った余りの足し算を入れる。

$$a * b \equiv a + b \pmod 3$$

このとき演算表は次のようになる。

$*$	0	1	2
0	0	1	2

1	1	2	0
2	2	0	1

全ての結果が S に入っているので閉包性がある。0 は単位元であり、1 の逆元は 2、2 の逆元は 1 である。

5　演習リンク

→ 基本演習 **代数的構造と二項演算** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/代数的構造と二項演算-基本演習/

6　まとめ

二項演算は、集合の二つの元から同じ集合の元を作る写像である。閉包性、結合法則、可換性、単位元、逆元は、群・環・体を定義するための基本語彙である。

7　判定補足：演算の性質は別々に確認する

集合 S と規則 $*$ が与えられたとき、まず $a,b\in S \Rightarrow a*b\in S$ を確認して、$*:S\times S\to S$ が二項演算 (binary operation) として定まっているかを見る。これは閉包性 (closure) だけの確認であり、結合法則、可換性、単位元、逆元はまだ保証しない。

たとえば $\mathbb{Z}$ 上の引き算 (subtraction) $a*b=a-b$ は閉包性 (closure) を持つが、

$$(5-3)-1=1,\qquad 5-(3-1)=3$$

なので結合法則を満たさない。したがって、閉包性 (closure) があることと群に近い性質を持つことは別問題である。

data/lecture/math/abstract-algebra/同値関係と剰余類の基本-講義.n.md md 4eb6de5

同値関係と剰余類

equivalence relation　residue class

抽象代数 で商構造を作る前に、「どの元を同じものとして 扱 うか」を決める必要がある。そのための道具が同値関係である。

同値関係は、対象 を分類する規則である。分類された一つ一つの箱が 同値類 であり、同値類全体の 集合 が 商集合 である。

equivalence class

quotient set

→ 講義 **同値関係と分割** lecture math discrete-math

https://study.bem130.com/lecture/math/discrete-math/同値関係と分割-講義/

1 同値関係の三つの 条件

集合 X 上の関係 $\sim$ が同値関係であるとは、次を満たすことである。

$$x \sim x$$

$$x \sim y \Rightarrow y \sim x$$

$$x \sim y \text{ and } y \sim z \Rightarrow x \sim z$$

それぞれ、反射性、対称性、推移性である。

2 同値類

元 $a \in X$ の同値類を

$$[a] = \{x \in X \mid x \sim a\}$$

で定義する。同値類は、代表元 a そのものではなく、a と同じものとみなされる元全体の 集合 である。

代表元は名前であり、同値類が本体である。したがって、$a \sim b$ なら

$$[a] = [b]$$

である。

同値類を全部集めた集合を商集合という。つまり、商集合では元そのものではなく、同値類を新しい元として扱う。

quotient set

3 剰余類

整数で、n を固定する。整数 a, b に対して

$$a \sim b \iff n \mid (a-b)$$

と定める。これは同値関係である。このとき a の同値類

$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$$

を剰余類という。

residue class

たとえば $n = 5$ のとき、

$$[2]_5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$

である。これらは全て 5 で割った余りが 2 である。

4 well-defined の問題

well-defined

商集合の上で演算を定義するとき、代表元の選び方に依存してはいけない。この性質を well-defined という。

well-defined

たとえば剰余類で

$$[a] + [b] = [a + b]$$

と定義したいなら、a を同じ類の別の代表元 a' に変え、b を同じ類の別の代表元 b' に変えても、結果の類が同じであることを確認する必要がある。

この確認を省くと、商集合の上の演算が実は定まっていない可能性がある。

5 演習リンク

→ 基本演習 **同値関係と合同式** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/同値関係と合同式-基本演習/

6 まとめ

同値関係は、元を分類する規則である。剰余類は整数を余りで分類した同値類であり、合同式と商環の基礎になる。 商集合 で演算するには、代表元によらず結果が定まることを必ず確認する。

7 証明補足：合同関係が同値関係である理由

整数 a, b に対して

$$a \sim b \iff n \mid (a-b)$$

と定める。ただし n は正の整数とする。この関係が同値関係であることを確認する。
equivalence relation

反射性は、$a-a=0$ が n で割り切れることから従う。対称性は、$n \mid (a-b)$ なら $b-a=-(a-b)$ も n で割り切れることから従う。推移性は、$n \mid (a-b)$ かつ $n \mid (b-c)$ なら

$$a-c=(a-b)+(b-c)$$

も n で割り切れることから従う。

したがって、合同であることは整数を剰余類へ分類する正当な同値関係である。

8 注意：well-defined でない定義の例

$\mathbb{Z}/2\mathbb{Z}$ で、剰余類 $[a]$ から整数 a そのものを返す写像を作ろうとすると失敗する。なぜなら $[0]=[2]$ だが、代表元を 0 と選ぶと 値 は 0、2 と選ぶと 値 は 2 になるからである。

商集合の元は代表元ではなく類である。類に対して何かを定義するときは、代表元を変えても同じ値になることを必ず確認する。

合同式と mod 演算

congruence　operation

合同式を「余りが同じ」という計算規則だけで見ると、何故足し算や掛け算が正当化されるのかが見えにくい。抽象代数では、合同式を剰余類の等号として見る。

$$a \equiv b \pmod{n}$$

とは、

$$n \mid (a-b)$$

という意味であり、同時に a と b が同じ剰余類に属するという意味でもある。

→ 講義 **同値関係と剰余類の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/同値関係と剰余類の基本-講義/

1　剰余類全体

$n \geq 2$ とする。整数全体を n で割った余りによって分類すると、商集合

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

が得られる。この集合の元は整数ではなく、整数の同値類である。

ここでの商集合とは、同じ余りを持つ整数を一つの類にまとめ、その類を元として扱う集合である。

2　足し算と掛け算

剰余類の加法と乗法を

$$[a] + [b] = [a+b]$$

$$[a][b] = [ab]$$

で定義する。

ここで重要なのは、右辺が代表元の選び方によらないことである。もし $a \equiv a' \pmod{n}$、$b \equiv b' \pmod{n}$ なら、

$$(a+b)-(a'+b') = (a-a')+(b-b')$$

は n の倍数である。また、

$$ab - a'b' = a(b-b') + b'(a-a')$$

も n の倍数である。したがって和と積は well-defined である。

well-defined

3 逆元がある条件

剰余類 $[a]$ が 乗法逆元 を持つとは、ある $[x]$ が存在して

$$[a][x] = [1]$$

となることである。これは

$$ax \equiv 1 \pmod{n}$$

と同じである。

この合同式が解を持つための 条件 は

$$\gcd(a, n) = 1$$

である。これは一次不定方程式

$$ax + ny = 1$$

が整数解を持つ 条件 と同じである。

→ 講義 **ユークリッドの互除法と一次不定方程式** lecture math algebra

https://study.bem130.com/lecture/math/algebra/ユークリッドの互除法と一次不定方程式-講義/

ここでは文字で割り算をするのではなく、最大公約数が 1 であることから逆元の存在を示している。したがって、割る操作を 行 う場面では、逆元が存在する 条件 を先に確認する必要がある。

4　フェルマーの小定理への接続

p が素数なら、0 でない剰余類は全て逆元を持つ。したがって

$$(\mathbb{Z}/p\mathbb{Z})^{\times}$$

は乗法について群になる。この群の構造から、$p \nmid a$ のとき

$$a^{p-1} \equiv 1 \pmod{p}$$

が導かれる。これがフェルマーの小定理である。

この節は後の群とラグランジュの定理への見通しである。このページの本流では、剰余類の演算が well-defined であることと、逆元の存在条件だけを使う。

5　証明補足：合同式が加法と乗法で保存される理由

n を正の整数とする。合同式

$$a \equiv b \pmod{n}, \qquad c \equiv d \pmod{n}$$

が成り立つなら、

$$a + c \equiv b + d \pmod{n}, \qquad ac \equiv bd \pmod{n}$$

である。

加法について証明する。$a \equiv b \pmod{n}$ は $n \mid (a-b)$、$c \equiv d \pmod{n}$ は $n \mid (c-d)$ という意味である。

したがって

$$(a+c) - (b+d) = (a-b) + (c-d)$$

も n で割り切れる。よって $a + c \equiv b + d \pmod{n}$ である。

乗法については

$$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d)$$

と変形する。$n \mid (a-b)$ かつ $n \mid (c-d)$ なので、右辺の二つの項はどちらも n で割り切れる。したがって $n \mid (ac-bd)$ であり、$ac \equiv bd \pmod{n}$ である。

ここでは n で割るのではなく、n が差を割り切ることを使っている。したがって文字式の除算に伴う 0 除算の問題は生じない。ただし、$\pmod{n}$ の記法では n を正の整数として固定している。

6 演習リンク

→ 基本演習 **同値関係と合同式** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/同値関係と合同式-基本演習/

7 まとめ

合同式は、剰余類の等号である。mod 演算が正当化されるのは、剰余類上の加法と乗法が代表元によらず定まるからである。乗法逆元は常にあるわけではなく、$\gcd(a,n)=1$ が必要である。

data/lecture/math/abstract-algebra/半群・モノイド・群への入口-講義.n.md md b57221b

半群・モノイド・群への入口

semigroup　monoid　group

群の定義をいきなり四条件で覚えると、何故その条件が必要なのかが見えにくい。そこで、二項演算に条件を一つずつ足していく。

$$\text{二項演算} \longrightarrow \text{半群} \longrightarrow \text{モノイド} \longrightarrow \text{群}$$

という流れで見ると、群は「演算を繰り返せて、何もしない操作があり、さらに戻せる構造」であることが分かる。

1　半群

半群とは、集合 S と結合法則を満たす二項演算 $*$ の組である。

semigroup

$$(a * b) * c = a * (b * c)$$

半群では、単位元や逆元は要求しない。結合法則があるため、長い積

$$a_1 * a_2 * \cdots * a_n$$

の括弧を 省略 できる。

2　モノイド

モノイドとは、単位元を持つ半群である。つまり、ある元 e が存在して、任意の a について

monoid

$$e * a = a * e = a$$

が成り立つ。

たとえば自然数全体 $\mathbb{N}$ は、足し算について 0 を単位元とするモノイドである。ただし自然数の範囲では、全ての元に加法逆元があるわけではないので群ではない。

3 群

群とは、全ての元が逆元を持つモノイドである。任意の a に対して、ある a^{-1} が存在して
group

$$a * a^{-1} = a^{-1} * a = e$$

となる。

群では、演算によって進んだ操作を逆元で戻せる。この「戻せる」性質が、群を対称性や変換の数学にしている。

4 具体例：自然数、整数、有理数

足し算で見ると、

$$(\mathbb{N}, +)$$

はモノイドである。0 は単位元だが、たとえば 3 を足して 0 に戻す自然数は存在しない。

$$(\mathbb{Z}, +)$$

は群である。整数 a の逆元は $-a$ である。

掛け算で見ると、

$$(\mathbb{Q} \setminus \{0\}, \cdot)$$

は群である。0 を除く理由は、0 には 乗法逆元 が存在しないからである。

5 何が変わり、何が保存されるか

半群からモノイドへ進むと、「何もしない操作」が使えるようになる。モノイドから群へ進むと、「戻す操作」が使えるようになる。一方で、いずれも演算が同じ 集合 の中で閉じていることと、結合法則は保存される。

6 演習リンク

→ 基本演習 **群と部分群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/群と部分群-基本演習/

7 まとめ

半群は結合法則を持つ演算、モノイドは単位元を持つ半群、群は全ての元に逆元があるモノイドである。この階段を理解すると、群の公理が必要最小限の条件として見える。

8 反例補足：半群・モノイド・群の階層は真に異なる

半群、モノイド、群は条件を一つずつ足していく階層である。ただし、上の概念が下の概念と同じになるわけではない。

$(\mathbb{Z}_{>0}, +)$ は結合法則を満たすので半群 (semigroup) である。しかし単位元 0 が $\mathbb{Z}_{>0}$ に入っていないのでモノイドではない。

$(\mathbb{Z}_{\geq 0}, +)$ は 0 を単位元に持つのでモノイド (monoid) である。しかし 1 の加法逆元 -1 が $\mathbb{Z}_{\geq 0}$ に入っていないので群ではない。

$(\mathbb{Z}, +)$ は 0 とすべての加法逆元を持つので群である。このように、各段階で新しく要求した条件が本当に効いている。

群の基本

group

群は、操作を合成し、必要なら元に戻せる構造である。整数の足し算、剰余類の足し算、図形の回転、可逆行列の積は見た目が違う。しかし、どれも同じ四つの条件を満たす。

1 群の定義

集合 G と二項演算 $*$ の組 $(G, *)$ が群であるとは、次を満たすことである。

$$a, b \in G \Rightarrow a * b \in G$$

$$(a * b) * c = a * (b * c)$$

$$\exists e \in G \text{ such that } e * a = a * e = a$$

$$\forall a \in G, \exists a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e$$

それぞれ、閉包性、結合法則、単位元、逆元である。

2 何故この四条件か

閉包性は、演算の結果が同じ世界に残ることを保証する。結合法則は、操作を何回も続けるときに括弧の位置を気にしなくてよいことを保証する。単位元は何もしない操作であり、逆元は操作を取り消す操作である。

この四条件があると、方程式

$$a * x = b$$

を

$$x = a^{-1} * b$$

と解ける。ここでは a^{-1} の存在を使っているため、逆元が存在することが不可欠である。

3 可換群

全ての $a, b \in G$ について

$$a * b = b * a$$

が成り立つ群を可換群という。整数の足し算は可換である。一方、置換の合成や行列積は一般に可換でない。

abelian group

→ 講義 **行列の積の意味** lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/行列の積の意味-講義/

ここでは、置換は集合の元を入れ替える操作、行列積は非可換な演算の例としてだけ使う。

4 基本例

群	演算	単位元	逆元
$(\mathbb{Z}, +)$	加法	0	$-a$
$(\mathbb{Z}/n\mathbb{Z}, +)$	剰余類の加法	$[0]$	$[-a]$
$(\mathbb{R}^\times, \cdot)$	乗法	1	$1/a$
S_n	置換の合成	恒等置換	逆置換
$GL_n(\mathbb{R})$	行列積	単位行列	逆行列

$\mathbb{R}^\times$ は 0 でない実数全体である。0 を除くのは、0 に乗法逆元がないからである。

S_n は $\{1, \ldots, n\}$ から自分自身への全単射、つまり置換の全体である。$GL_n(\mathbb{R})$ は積に関して逆元を持つ $n \times n$ 実行列の全体である。行列の詳しい計算は、このページの証明の前提にはしない。

5 何を変えて何を保存するか

群として見ると、元の具体的な姿は重要でなくなる。整数、置換、行列は別物である。しかし、演算を繰り返せること、単位元があること、逆元で戻せることは共通している。この共通構造を保存して議論するのが群論である。

6 証明補足：単位元・逆元・消去法則

群 (group) では、単位元は一意である。e と e' がどちらも単位元だとする。e は単位元なので $ee' = e'$ であり、e' は単位元なので $ee' = e$ である。したがって $e = e'$ である。

逆元も一意である。b と c がどちらも a の逆元だとする。つまり $ab = e$、$ca = e$ である。このとき

$$b = eb = (ca)b = c(ab) = ce = c$$

である。ここで結合法則を使っている。

さらに、群では消去法則 (cancellation law) が成り立つ。

$$ab = ac \implies b = c$$

である。実際、左から a^{-1} を掛けると

$$a^{-1}(ab) = a^{-1}(ac)$$

である。結合法則より $(a^{-1}a)b = (a^{-1}a)c$、つまり $eb = ec$ となる。したがって $b = c$ である。

この証明は、群で「逆に戻せる」ことが、方程式を解く力になっていることを示している。

7 演習リンク

→ 基本演習 **群と部分群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/群と部分群-基本演習/

8 まとめ

群は、閉包性、結合法則、単位元、逆元を持つ代数的構造である。群を学ぶ理由は、数・置換・行列・対称性を同じ言葉で扱うためである。

data/lecture/math/abstract-algebra/部分群と生成-講義.n.md md ef2b946

部分群と生成

subgroup generation

群の中に、群としての構造を保った小さな部分を見つけたいことがある。そのような部分集合が部分群である。

部分群は、単なる部分集合ではない。元どうしを演算しても中に残り、逆元も中に残る必要がある。

1 部分群の定義

群 G の部分集合 $H \subseteq G$ が部分群であるとは、H が G の演算を受け継いで群になることである。

実用上は、次の条件で判定できる。

$$H \neq \emptyset$$

かつ、任意の $a, b \in H$ について

$$ab^{-1} \in H$$

が成り立つなら、H は部分群である。

この判定では割り算をしているように見えるが、群の中で逆元 b^{-1} が存在することを使っている。したがって、b が群の元であることと、逆元が群の中にあることが前提である。

2 具体例

$(\mathbb{Z}, +)$ の中で、偶数全体

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$$

は部分群である。0 を含み、偶数どうしの差は偶数だからである。

一方、自然数全体 $\mathbb{N}$ は $(\mathbb{Z}, +)$ の部分群ではない。たとえば 3 は含むが、逆元 -3 を含まない。

3 生成元

群 G の部分集合 A から、A の元とその逆元を有限回演算して得られる元全体を、A が生成する部分群という。

$$\langle A \rangle$$

と書く。

一つの元 a で生成される群

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

を巡回群という。
cyclic group

4 例：剰余類の巡回群

$(\mathbb{Z}/6\mathbb{Z}, +)$ では、$[1]$ は全体を生成する。

$$[0], [1], [2], [3], [4], [5]$$

が $[1]$ の繰り返しで得られるからである。一方、$[2]$ が生成する部分群は

$$\{[0], [2], [4]\}$$

である。

5 何が保存されるか

部分群では、元の群の演算、単位元、逆元がそのまま保たれる。変わるのは、使える元の範囲である。生成では、少数の元から閉包性と逆元を使って、必要最小限の部分群を作る。

6　証明補足：部分群判定法と生成部分群の最小性

G を群、$H \subseteq G$ を空でない部分集合とする。もし

$$x, y \in H \implies xy^{-1} \in H$$

が成り立つなら、H は部分群 (subgroup) である。

証明する。H は空でないので、ある $h \in H$ が存在する。すると $hh^{-1} = e \in H$ である。つぎに $x \in H$ とする。$e \in H$ なので、条件を e, x に使うと $ex^{-1} = x^{-1} \in H$ である。最後に $x, y \in H$ とする。いま $y^{-1} \in H$ が分かっているので、条件を x, y^{-1} に使うと $x(y^{-1})^{-1} = xy \in H$ である。よって H は単位元、逆元、積について閉じている。

生成部分群 $\langle S \rangle$ は、S を含むすべての部分群の共通部分として定義できる。

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

この共通部分は部分群である。なぜなら、単位元はすべての H に含まれ、積と逆元も各 H の中で閉じているからである。また、どの H も S を含むので、共通部分も S を含む。さらに S を含む任意の部分群 K は、交わりを取る対象の一つなので、$\langle S \rangle \subseteq K$ である。よって $\langle S \rangle$ は S を含む最小の部分群である。

7　演習リンク

→ 基本演習 **群と部分群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/群と部分群-基本演習/

8　まとめ

部分群は、群の構造を保ったまま元を制限したものである。生成は、指定した元から閉じた最小の部分群を作る操作であり、巡回群は一つの元で生成される群である。

9 計算補足：$\mathbb{Z}/n\mathbb{Z}$ で $[k]$ が生成する部分群

加法群 $(\mathbb{Z}/n\mathbb{Z}, +)$ で $[k]$ が生成する部分群の元は

$$[0], [k], [2k], [3k], \ldots$$

である。この列が初めて $[0]$ に戻る正の整数 m は、$n \mid mk$ を満たす最小の m である。したがって $d = \gcd(n, k)$ とすると

$$| \langle [k] \rangle | = \frac{n}{d}$$

である。

たとえば $\mathbb{Z}/12\mathbb{Z}$ で $[8]$ を考えると、$\gcd(12, 8) = 4$ なので生成される部分群の位数は $12/4 = 3$ である。実際、

$$\langle [8] \rangle = \{[0], [8], [4]\}$$

である。

data/lecture/math/abstract-algebra/剰余類とラグランジュの定理-講義.n.md md a113a4d

剰余類とラグランジュの定理

coset

整数の剰余類は、整数を余りで分類するものだった。群でも、部分群を基準にして元を分類できる。その分類が群の剰余類である。

1 左剰余類

群 G の部分群 H と元 $g \in G$ に対して、

$$gH = \{gh \mid h \in H\}$$

を H の左剰余類という。

left coset

右から掛ける

$$Hg = \{hg \mid h \in H\}$$

を右剰余類という。

right coset

群が可換なら左剰余類と右剰余類は一致する。しかし一般の群では一致するとは限らない。

2 剰余類は群を分割する

左剰余類どうしは、等しいか交わらないかのどちらかである。また、全ての左剰余類を集めると G 全体を覆う。

これは、剰余類が G を同じ大きさの箱に分けることを意味する。

3 ラグランジュの定理

有限群 G と部分群 H に対して、

$$|G| = [G : H]|H|$$

が成り立つ。ここで $[G : H]$ は H の左剰余類の個数である。

したがって、

$$|H| \mid |G|$$

である。これがラグランジュの定理である。
Lagrange's theorem

4 具体例

$G = \mathbb{Z}/6\mathbb{Z}$、$H = \{[0], [3]\}$ とする。H の位数は 2 である。剰余類は

$$[0] + H = \{[0], [3]\}$$
$$[1] + H = \{[1], [4]\}$$
$$[2] + H = \{[2], [5]\}$$

の三つである。したがって $|G| = 6 = 3 \cdot 2$ である。

5 何が保存されるか

剰余類に分けると、個々の元ではなく、部分群だけずれたものを同じ箱として見る。部分群の大きさは各箱で保存される。これにより、有限群の位数が部分群の位数で割り切れることが分かる。

6 商群への注意

剰余類の集合はいつでも作れる。しかし、剰余類どうしの積で群を作れるとは限らない。商群を作るには、部分群が正規部分群である必要がある。

→ 講義 **正規部分群と商群** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/正規部分群と商群-講義/

7　証明補足：剰余類の分割とラグランジュの定理

$H \leq G$ とする。左剰余類 aH と bH は、交わらないか、完全に一致する。

証明する。$aH \cap bH \neq \emptyset$ とし、$x \in aH \cap bH$ を取る。すると $x = ah_1 = bh_2$ となる $h_1, h_2 \in H$ が存在する。

ここから

$$b^{-1}a = h_2 h_1^{-1} \in H$$

である。任意の $ah \in aH$ について、

$$ah = b(b^{-1}a)h$$

であり、$(b^{-1}a)h \in H$ だから $ah \in bH$ である。よって $aH \subseteq bH$ である。同じ議論で $bH \subseteq aH$ も従うので $aH = bH$ である。

また、写像

$$H \to aH, \qquad h \mapsto ah$$

は全単射である。全射は aH の定義から従う。単射は、$ah_1 = ah_2$ なら左から a^{-1} を掛けて $h_1 = h_2$ となることから従う。ここでは a^{-1} が存在すること、つまり G が群であることを使っている。

したがって、有限群 G では、G は同じ大きさの左剰余類に分割される。左剰余類の個数を $[G : H]$ とすれば

$$|\, G \,| = [G : H] |\, H \,|$$

である。これがラグランジュの定理 である。
Lagrange's theorem

8　演習リンク

→ 基本演習 **剰余類・正規部分群・商群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/剰余類・正規部分群・商群-基本演習/

9 まとめ

群の剰余類は、部分群を基準に群を同じ大きさの箱へ分ける方法である。有限群では、部分群の位数は群の位数を割り切る。商群を作るには、さらに正規性が必要である。

10 系：元の位数は群の位数を割り切る

有限群 G の元 g が生成する部分群 $\langle g \rangle$ を考える。ラグランジュの定理より、

$$| \langle g \rangle | \mid | G |$$

である。$| \langle g \rangle |$ は g の位数なので、有限群では各元の位数が群の位数を割り切る。

特に、$| G | = p$ が素数なら、単位元でない元 g の位数は 1 ではなく、p を割り切るので p である。したがって $G = \langle g \rangle$ であり、位数が素数の群は巡回群である。

data/lecture/math/abstract-algebra/正規部分群と商群-講義.n.md md 62a31e5

正規部分群と 商群

normal subgroup　quotient group

剰余類の集合を作るだけなら、任意の部分群でよい。しかし、剰余類どうしを掛けて再び剰余類にしたいなら、代表元の選び方に依存しない必要がある。この条件を満たす部分群が正規部分群である。

1 正規部分群の定義

部分群 $N \leq G$ が正規部分群であるとは、任意の $g \in G$ について

$$gN = Ng$$

が成り立つことである。このとき

$$N \trianglelefteq G$$

と書く。

同値な条件として、任意の $g \in G$、$n \in N$ について

$$gng^{-1} \in N$$

が成り立つことでもよい。

2 何故正規性が必要か

剰余類の積を

$$(gN)(hN) = (gh)N$$

で定義したい。この定義が代表元によらないためには、g や h を同じ剰余類の別の元に取り替えても、結果が同じ剰余類になる必要がある。

正規性は、この well-defined 性を保証する条件である。

well-defined

3 商群

$N \trianglelefteq G$ のとき、剰余類全体

$$G/N = \{gN \mid g \in G\}$$

は、積

$$(gN)(hN) = (gh)N$$

によって群になる。これを商群という。

商群では、N に属する違いを 0 のように潰して見る。つまり、N の中で動く差を無視して、残った構造だけを調べる。

4 具体例：整数の商群

$(\mathbb{Z}, +)$ において、$n\mathbb{Z}$ は正規部分群である。何故なら $\mathbb{Z}$ は可換群だから、全ての部分群が正規である。

商群

$$\mathbb{Z}/n\mathbb{Z}$$

は、整数を n で割った余りで分類した群である。

5 何を変えて何を保存するか

商群では、N の中の違いを見ない。変わるのは元の粒度であり、個々の元ではなく剰余類を元として扱う。
一方で、群の演算構造は well-defined な形で保存される。

well-defined

6 証明補足：商群の演算が well-defined になる条件

$N \leq G$ とする。剰余類どうしの積を

$$(aN)(bN) = (ab)N$$

で定義したい。この定義が代表元の選び方に依存しないためには、N が正規部分群 (normal subgroup) であることが必要である。

まず N が正規だとする。$aN = a'N$、$bN = b'N$ とする。このとき $a' = an_1$、$b' = bn_2$ となる $n_1, n_2 \in N$ が存在する。すると

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2$$

である。N は正規なので $b^{-1}n_1b \in N$ であり、したがって $(b^{-1}n_1b)n_2 \in N$ である。よって $a'b'N = abN$ である。つまり積は代表元に依存しない。

逆に、この積が常に well-defined だとする。任意の $g \in G$ と $n \in N$ を取る。左剰余類として $(gn)N = gN$ なので、第一因子の代表元を g から gn に替えても、$g^{-1}N$ との積は同じでなければならない。したがって

$$(gN)(g^{-1}N) = N, \qquad ((gn)N)(g^{-1}N) = gng^{-1}N$$

が同じ剰余類になる。よって $gng^{-1}N = N$、すなわち $gng^{-1} \in N$ である。任意の g, n について成り立つので、N は正規である。

つまり、正規性は「剰余類を要素として掛けても矛盾しない」ことを保証する条件である。

7 演習リンク

→ 基本演習 **剰余類・正規部分群・商群** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/剰余類・正規部分群・商群-基本演習/

8 まとめ

正規部分群は、剰余類の集合に群構造を入れるための条件である。商群は、正規部分群の中の違いを潰して残る構造を見る方法である。

9 反例：すべての部分群が正規とは限らない

対称群 S_3 で、$H = \{e, (12)\}$ を考える。これは部分群である。しかし $g = (13)$ とすると、

$$gH = \{(13), (13)(12)\}$$

であり、

$$Hg = \{(13), (12)(13)\}$$

である。ここで $(13)(12)$ と $(12)(13)$ は異なる置換である。したがって $gH \neq Hg$ であり、H は正規部分群ではない。

この例では剰余類の集合は作れるが、剰余類どうしの積を代表元によらず定義できない。つまり、非可換な群では正規性の確認が本質的である。

data/lecture/math/abstract-algebra/群準同型と同型-講義.n.md md 2b20198

群準同型 と 同型

group homomorphism　isomorphism

群どうしを比べるとき、元の名前が一致する必要はない。重要なのは、演算の構造が保たれることである。
この「演算を保つ写像」が群準同型である。

1 群準同型

群 G, H に対して、写像 $\varphi : G \to H$ が群準同型であるとは、任意の $a, b \in G$ について

$$\varphi(ab) = \varphi(a)\varphi(b)$$

が成り立つことである。

ここで左辺の積は G の演算であり、右辺の積は H の演算である。記号が同じでも、どの群の演算かを区別する必要がある。

2 準同型が自動的に保つもの

群準同型 $\varphi : G \to H$ は単位元を単位元へ送る。

$$\varphi(e_G) = e_H$$

また、逆元を逆元へ送る。

$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

これらは定義に直接書かれていないが、演算を保つことから導かれる。

3 核と像

群準同型 $\varphi : G \to H$ の核を
kernel

$$\ker \varphi = \{ g \in G \mid \varphi(g) = e_H \}$$

で定義する。核は、写像によって単位元に潰れる部分である。

像は
image

$$\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$$

である。像は、実際に到達する元全体である。

4 同型

群準同型 $\varphi : G \to H$ が全単射であるとき、群同型という。このとき G と H は群として同じ構造を持つ。

$$G \cong H$$

と書く。

同型では、元の名前は変わる。しかし、演算表、単位元、逆元、部分群の構造、位数などの群論的性質は保存される。

5 具体例

$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を

$$\varphi(k) = [k]$$

で定める。これは群準同型である。

$$\varphi(a+b) = [a+b] = [a] + [b]$$

だからである。この写像の核は

$$\ker\varphi = n\mathbb{Z}$$

である。

6 証明補足：準同型が保存するもの

$\varphi : G \to H$ を群準同型 (group homomorphism) とする。このとき

$$\varphi(e_G) = e_H, \qquad \varphi(g^{-1}) = \varphi(g)^{-1}$$

である。

まず $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ である。左から $\varphi(e_G)^{-1}$ を掛けると $e_H = \varphi(e_G)$ である。つぎに

$$e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

なので、$\varphi(g^{-1})$ は $\varphi(g)$ の逆元である。よって $\varphi(g^{-1}) = \varphi(g)^{-1}$ である。

さらに、核 (kernel) $\ker\varphi$ は G の正規部分群である。$a, b \in \ker\varphi$ なら

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H^{-1} = e_H$$

なので $ab^{-1} \in \ker\varphi$ であり、部分群判定法から部分群である。また $g \in G$、$a \in \ker\varphi$ について

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H$$

なので $gag^{-1} \in \ker\varphi$ である。したがって核は正規である。

最後に、φ が単射であることと $\ker\varphi = \{e_G\}$ は同値である。φ が単射なら、$\varphi(g) = e_H = \varphi(e_G)$ から $g = e_G$ である。逆に $\ker\varphi = \{e_G\}$ とし、$\varphi(g_1) = \varphi(g_2)$ とする。すると

$$\varphi(g_1 g_2^{-1}) = e_H$$

なので $g_1 g_2^{-1} \in \ker\varphi$、したがって $g_1 g_2^{-1} = e_G$ である。よって $g_1 = g_2$ であり、φ は単射である。

7 演習リンク

→ 基本演習 **準同型と同型** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/準同型と同型-基本演習/

8 まとめ

群準同型は演算を保つ写像である。核は潰れる部分、像は到達する部分である。同型は構造を完全に保存する準同型であり、抽象代数で「本質的に同じ」を表す。

data/lecture/math/abstract-algebra/群作用と対称性-講義.n.md md 054692a

群作用と対称性

group action　symmetry

群は、単なる演算表としてだけでなく、集合を動かす 変換 の集まりとして見ることができる。この見方が群作用である。

群作用を使うと、「群の 元 が 対象 をどう動かすか」を 直接 扱 える。図形の回転、 置換 、 行列 による線型変換は、全て群作用の例である。

→ 講義 線型写像と行列 lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/線型写像と行列-講義/

線型変換は応用例としての見通しである。このページの定義と 証明 では、集合 の元を別の元へ移す変換だけを使う。

1 群作用の定義

群 G が集合 X に作用するとは、各 $g \in G$ と $x \in X$ に対して 元 $g \cdot x \in X$ が定まり、次を満たすことである。

$$e \cdot x = x$$

$$(gh) \cdot x = g \cdot (h \cdot x)$$

第一式は、単位元は何もしないことを 表す。第二式は、群の 積 と 変換 の 合成 が対応することを 表す。

2 軌道

元 $x \in X$ の軌道を

$$Gx = \{g \cdot x \mid g \in G\}$$

で定義する。軌道は、群の作用によって x から到達できる元全体である。

3　固定部分群

元 $x \in X$ を動かさない群の元全体

$$G_x = \{g \in G \mid g \cdot x = x\}$$

を固定部分群という。これは G の部分群である。

stabilizer

軌道は「どこへ動けるか」を表し、固定部分群は「何が変わらないか」を表す。

4　具体例：正三角形の対称性

正三角形の 頂点集合 を $X = \{1, 2, 3\}$ とする。正三角形の回転と反転の 対称性 は、頂点集合 を置換する。したがって、対称性の群は X に作用する。

頂点 1 の軌道は $\{1, 2, 3\}$ である。どの 頂点 にも 対称性 で移れるからである。一方、 頂点 1 を固定する 対称性 は、恒等変換と、 頂点 1 を通る軸での反転である。

5　何を変えて何を保存するか

群作用では、群の元を変換として見る。変わるのは集合の元の位置である。保存されるのは、群の積と変換の合成が対応するという構造である。

群作用の 考え方は、幾何、線型代数、物理、組合せ論に広く 現れる。

6　演習リンク

→ 基本演習 **準同型と同型** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/準同型と同型-基本演習/

7 まとめ

群作用は、群を集合上の変換として見る方法である。軌道は動ける範囲、固定部分群は動かさない対称性を表す。群作用によって、抽象的な群を具体的な変換として理解できる。

8 定理：軌道・固定部分群定理

有限群 G が集合 X に作用し、$x \in X$ とする。このとき

$$| Gx | = [G : G_x]$$

である。したがって G が有限なら

$$| G | = | Gx | | G_x|$$

が成り立つ。これを軌道固定部分群定理という。

orbit-stabilizer theorem

証明の考えは、剰余類と軌道を対応させることである。写像

$$G/G_x \to Gx, \qquad gG_x \mapsto g \cdot x$$

を考える。もし $gG_x = hG_x$ なら $h^{-1}g \in G_x$ なので $(h^{-1}g) \cdot x = x$ であり、$g \cdot x = h \cdot x$ である。したがって写像は well-defined である。逆に $g \cdot x = h \cdot x$ なら $h^{-1}g \in G_x$ なので $gG_x = hG_x$ である。よって全単射である。

ここで全単射とは、異なる 入力 を異なる 出力 へ送り、かつ目標の元を全て 出力 として得る写像である。有限集合では全単射があると元の個数が等しい。

正三角形の対称群では、頂点 1 の軌道は 3 個、固定部分群は 2 個の元を持つ。したがって群の位数は $3 \cdot 2 = 6$ である。

9 証明補足：軌道・固定部分群定理が成り立つ理由

群 G が集合 X に作用しているとし、$x \in X$ を固定する。x の固定部分群を $G_x = \{g \in G \mid g \cdot x = x\}$ と書く。

写像

$$G/G_x \to G\cdot x, \qquad gG_x \mapsto g\cdot x$$

を考える。この写像が well-defined であることを確認する。もし $gG_x = hG_x$ なら $h^{-1}g \in G_x$ である。したがって

$$(h^{-1}g)\cdot x = x$$

であり、左から h を作用させると $g\cdot x = h\cdot x$ である。よって代表元を変えても行き先は変わらない。

逆に $g\cdot x = h\cdot x$ なら $h^{-1}g\cdot x = x$ なので $h^{-1}g \in G_x$、したがって $gG_x = hG_x$ である。よってこの写像は単射かつ全射である。有限群の場合、

$$|\, G\cdot x \,| = [G : G_x] = \frac{|\, G \,|}{|\, G_x|}$$

が得られる。

data/lecture/math/abstract-algebra/環の基本-講義.n.md md 4fe62c2

環の基本

ring

群は一つの演算を持つ構造だった。環は、加法と 乗法 という二つの演算を同時に持つ構造である。

環を学ぶ目的は、整数、多項式、行列、剰余類を同じ言葉で扱うことである。これらは見た目は違うが、加法と 乗法 が分配法則で結びついている。

1 環の定義

集合 R と二つの演算 $+$、$\cdot$ の組 $(R, +, \cdot)$ が環であるとは、次を満たすことである。

まず、$(R, +)$ は可換群である。つまり、加法には 0 があり、各 元 a に加法逆元 $-a$ がある。

次に、 乗法 は閉じていて結合法則を満たす。

$$(ab)c = a(bc)$$

さらに、加法と 乗法 は分配法則で結ばれる。

$$a(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

乗法単位元 1 を要求する流儀も多い。この教材では、特に断らない限り、環は乗法単位元を持つものとして扱う。

2 何故 乗法逆元 を要求しないか

整数環 $\mathbb{Z}$ では、2 の 乗法逆元 は整数の中に存在しない。もし環の定義で 0 以外全てに 乗法逆元 を要求すると、整数を環として扱えなくなる。

環は、割り算までは要求しない。その代わり、足し算と掛け算が一緒に動く構造を保つ。

0 以外全てに 乗法逆元 を要求した可換環が体である。

→ 講義 **体の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/体の基本-講義/

3 基本例

環	加法	乗法	特徴
$\mathbb{Z}$	整数の加法	整数の乗法	割り算は一般に閉じない
$\mathbb{Z}/n\mathbb{Z}$	剰余類の加法	剰余類の乗法	合成数法では零因子が表れる
$F[x]$	多項式の加法	多項式の乗法	係数体 F 上の多項式環
$M_n(F)$	行列の加法	行列積	一般に非可換

行列積が非可換であるため、環では乗法の可換性を必ずしも要求しない。

→ 講義 **行列の積の意味** lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/行列の積の意味-講義/

$M_n(F)$ は非可換環の代表例として挙げている。行列の詳しい理論は、この章の環の定義には必要ない。

4 何が保存されるか

環では、加法の群構造、乗法の結合法則、分配法則が保存される。足し算だけを見ると群であり、掛け算だけを見るとモノイドに近い構造である。分配法則があるため、展開や因数分解のような計算ができる。

5 演習リンク

→ 基本演習 **環・イデアル・商環** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/環・イデアル・商環-基本演習/

6 まとめ

環は、加法と 乗法 を分配法則で結んだ代数的構造である。整数、多項式、剰余類、行列 を同じ言葉で 扱える。 乗法逆元 を全てに 要求 しないため、整数や多項式を自然に含められる。

7 補足：単元と体の違い

環 R の元 u が単元であるとは、ある $v \in R$ が存在して

$$uv = vu = 1$$

となることである。体では 0 以外の全ての元が単元である。しかし一般の環では、単元は一部の元だけである。

たとえば $\mathbb{Z}$ の単元は 1 と -1 だけである。2 は $\mathbb{Z}$ の元だが、$2v = 1$ となる整数 v は存在しない。したがって、環では「掛けられる」ことと「割れる」ことを区別する必要がある。

8 注意：可換でない環

行列環 $M_n(F)$ では、一般に $AB \neq BA$ である。このため、環の計算では乗法の順序を勝手に入れ替えてはいけない。可換環であることを使う議論では、その仮定を明示することが重要である。

data/lecture/math/abstract-algebra/イデアルと商環-講義.n.md md 51c5e16

イデアルと 商環

quotient ring

群で商群を作るには正規部分群が必要だった。環で商環を作るには、正規部分群に対応する役割を持つ部分集合が必要である。それがイデアルである。

ideal

1 イデアルの定義

環 R の部分集合 I がイデアルであるとは、$0 \in I$ であり、さらに次を満たすことである。

$$a, b \in I \Rightarrow a - b \in I$$

$$r \in R, a \in I \Rightarrow ra \in I \text{ and } ar \in I$$

$0 \in I$ により I は空ではない。第一条件は、I が加法について部分群であることを表す。第二条件は、環の任意の元を掛けても I の中に残ることを表す。

可換環では ra と ar は同じなので、片側だけ確認すればよい。

2 何故イデアルが必要か

商環では、I の元を 0 とみなす。つまり、a と b の差が I に属するとき、同じ元として扱う。

$$a \sim b \iff a - b \in I$$

この同値関係で作った同値類を使い、

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

と定義したい。この乗法が代表元によらず定まるために、イデアル条件が必要である。

ここでの同値類は $a + I = \{a + i \mid i \in I\}$ と書ける。商環では、これらの類全体を元として扱う。

3 整数の例

$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ は $\mathbb{Z}$ のイデアルである。

商環

$$\mathbb{Z}/n\mathbb{Z}$$

は、整数を n の倍数の差を無視してまとめたものである。これは合同式の世界そのものである。

→ 講義 **合同式と mod 演算の基本** lecture math abstract-algebra

https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-講義/

4 商群との対応

群論	環論
正規部分群	イデアル
商群	商環
群準同型の核	環準同型の核
第一同型定理	第一同型定理

どちらも、核として潰れる部分を 0 とみなして商を作るという点で同じである。

環準同型と第一同型定理は後で扱う。この表は、イデアルが後で核として現れるという見通しを示すためのものである。

5 何を変えて何を保存するか

商環では、イデアルの中の違いを 0 として潰す。変わるのは元の粒度である。一方で、加法、乗法、分配法則は商の上でも well-defined に保存される。

well-defined

6 証明補足：商環の演算が代表元によらない理由

I を環 R のイデアル とする。剰余類の和と積を

ideal

$$(a+I)+(b+I)=(a+b)+I, \qquad (a+I)(b+I)=ab+I$$

で定義する。この定義が代表元に依存しないことを証明する。

$a+I=a'+I$、$b+I=b'+I$ とする。これは $a'-a\in I$、$b'-b\in I$ という意味である。和については

$$(a'+b')-(a+b)=(a'-a)+(b'-b)\in I$$

なので $(a'+b')+I=(a+b)+I$ である。

積については

$$a'b'-ab=a'b'-a'b+a'b-ab=a'(b'-b)+(a'-a)b$$

である。$b'-b\in I$ であり、I は環の要素を掛けても I の中に残るので $a'(b'-b)\in I$ である。同じく $(a'-a)b\in I$ である。したがって $a'b'-ab\in I$ であり、$a'b'+I=ab+I$ である。

この証明から、イデアルの条件は「余りの類どうしを掛けても壊れない」ための条件だと分かる。

7 演習リンク

→ 基本演習 **環・イデアル・商環** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/環・イデアル・商環-基本演習/

8 まとめ

イデアルは、商環を作るための部分集合である。商環では、イデアルの元を 0 とみなし、残った剰余類に加法と乗法を入れる。整数の $\mathbb{Z}/n\mathbb{Z}$ は最も基本的な商環である。

data/lecture/math/abstract-algebra/整域・零因子・多項式環-講義.n.md md 1726d54

整域・零因子・多項式環

integral domain　zero divisor　polynomial ring

環では、0 でない二つの元を掛けた結果が 0 になることがある。この現象は、掛け算によって情報が潰れることを意味する。その原因になる元を零因子という。

1 零因子

環 R の 0 でない元 a が零因子であるとは、0 でない元 b が存在して

$$ab = 0$$

または

$$ba = 0$$

となることである。

たとえば $\mathbb{Z}/6\mathbb{Z}$ では、

$$[2][3] = [6] = [0]$$

である。[2] も [3] も 0 ではないので、零因子である。

2 整域

整域 (integral domain) とは、0 でない元どうしの積が 0 にならない可換環である。つまり、

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

が成り立つ。

整数環 $\mathbb{Z}$ は整域である。実数体 $\mathbb{R}$ も整域である。一方、$\mathbb{Z}/6\mathbb{Z}$ は整域ではない。

3 何故整域が重要か

整域では、0 でない元による掛け算で情報が潰れない。たとえば $a \neq 0$ のとき、

$$ab = ac \Rightarrow b = c$$

が成り立つ。実際、両辺を移項すると

$$a(b - c) = 0$$

であり、整域なので $b - c = 0$ である。

ここでは割り算を使っていない。0 でない元で割ったのではなく、零因子がないことを使って消去している。

4 多項式環

環 R 上の多項式全体

$$R[x]$$

は環になる。係数が体 F に属する場合、$F[x]$ は特に重要である。

$F[x]$ では、次数、割り算、既約多項式などを使って整数論に似た議論ができる。

→ 講義 **多項式** lecture math algebra

https://study.bem130.com/lecture/math/algebra/多項式-講義/

5 体との関係

体の正式な定義は次の講義で扱う。この節では先取りとして、体を「0 でない全ての元が乗法逆元を持つ可換環」として使う。

全ての体は整域である。何故なら、$a \neq 0$ で $ab = 0$ なら、a^{-1} を掛けて

$$b = 0$$

が導かれるからである。この場面では a^{-1} を使うため、$a \neq 0$ の確認が必要である。

6　証明補足：整域で消去法則が成り立つ理由

整域（integral domain）では、$a \neq 0$ かつ $ab = ac$ なら $b = c$ である。

証明する。$ab = ac$ から

$$ab - ac = 0$$

である。分配法則より

$$a(b - c) = 0$$

である。$a \neq 0$ であり、整域には零因子がないので、$b - c = 0$ でなければならない。よって $b = c$ である。

ここで文字式の割り算は使っていない。a で割るのではなく、「$a \neq 0$ で $a(b-c) = 0$ なら $b - c = 0$」という零因子の不存在を使っている。体での消去は逆元で掛ける方法でも説明できるが、整域ではこの証明の方が本質である。

7　演習リンク

→ 基本演習 **整域・体・有限体** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/整域・体・有限体-基本演習/

8　まとめ

零因子は、0 でない元どうしの積を 0 にしてしまう元である。整域ではそのような潰れが起きない。多項式環は、環論と代数・整数論をつなぐ基本的な例である。

9 定理：整域上の多項式環も整域

R が 整域 (integral domain) なら、$R[x]$ も整域である。

証明する。0 でない多項式 $f(x), g(x) \in R[x]$ を取る。f の最高次の係数を a、g の最高次の係数を b とする。

f, g は 0 でないので $a \neq 0$、$b \neq 0$ である。R は整域なので $ab \neq 0$ である。

積 fg の最高次の係数は ab なので、fg は 0 多項式ではない。したがって 0 でない多項式どうしの積は 0 にならず、$R[x]$ は整域である。

この定理により、体 F 上の多項式環 $F[x]$ では次数を使った議論が安定する。

data/lecture/math/abstract-algebra/体の基本-講義.n.md md 9cc4067

体の基本

field

体は、0 以外の 元 で割り算ができる 可換環 である。体を学ぶ理由は、方程式、線型代数、多項式の計算を安定して行うためである。

整数では $2x = 1$ を整数の中で解けない。しかし有理数や実数では $x = 1/2$ と解ける。この違いを構造として表したものが体である。

1 体の定義

field

可換環 F が体であるとは、$0 \neq a \in F$ の任意の 元 が 乗法逆元 を持つことである。

$$\forall a \in F, a \neq 0 \Rightarrow \exists a^{-1} \in F \text{ such that } aa^{-1} = 1$$

ここで 0 を除くことが重要である。0 に 乗法逆元 は存在しない。もし $0b = 1$ となる b があれば、左辺は 0 なので矛盾する。

2 基本例

$$\mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}$$

は体である。

一方、$\mathbb{Z}$ は体ではない。2 の 乗法逆元 $1/2$ が整数ではないからである。

また、p が 素数 のとき

$$\mathbb{Z}/p\mathbb{Z}$$

は体である。0 でない剰余類 $[a]$ について、$\gcd(a, p) = 1$ なので 逆元 が存在する。

3 体上で線型代数が動く理由

field　linear algebra

線型代数では、係数を割る操作が頻繁に表れる。たとえば掃き出し法では、主成分を 1 にするために 0 でない数で割る。

linear algebra　Gaussian elimination　pivot

→ 講義 行基本変形の基本 lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/行基本変形の基本-講義/

この操作が正当化されるのは、係数が体の元であり、0 でない元に逆元が存在するからである。

field　element　element　inverse element

この節は応用への見通しであり、線型代数の結果を以後の体の定義や証明の前提にはしない。

4 体と整域

field　integral domain

全ての体は整域である。何故なら、$ab = 0$ かつ $a \neq 0$ なら、a^{-1} を掛けて

$$b = 0$$

が導かれるからである。この議論では $a \neq 0$ を使っている。0 で割っているわけではなく、0 でない元の逆元を使っている。

element　inverse element

逆に、全ての整域が体であるわけではない。$\mathbb{Z}$ は整域だが体ではない。

integral domain　field　integral domain　field

5 何が変わり、何が保存されるか

環から体へ進むと、0 以外の元で割り算ができるようになる。保存されるのは、加法、乗法、分配法則、可換性である。追加されるのは、0 以外の乗法逆元である。

ring　field　element　addition　multiplication　distributive law　commutativity　multiplicative inverse

6 証明補足：体は整域である

field　integral domain

体は零因子を持たない。つまり、$ab = 0$ なら $a = 0$ または $b = 0$ である。

field　zero divisor

証明する。$ab = 0$ とし、$a \neq 0$ と仮定する。体（field）では 0 でない要素 a に 逆元（inverse element） a^{-1} が存在する。左から a^{-1} を掛けると

$$a^{-1}(ab) = a^{-1}0$$

である。結合法則より $(a^{-1}a)b = 0$、つまり $b = 0$ である。したがって $ab = 0$ なら $a = 0$ または $b = 0$ である。

ここでは $a \neq 0$ を確認してから a^{-1} を使っている。$a = 0$ の場合はすでに結論が成り立つので、逆元（inverse element） を使う必要がない。

7　演習リンク

→ 基本演習 **整域・体・有限体** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/整域・体・有限体-基本演習/

8　まとめ

体（field）は、0 以外の 元（element） に 乗法逆元（multiplicative inverse） がある 可換環（commutative ring） である。割り算ができるため、方程式や線型代数（linear algebra）の基本操作が自然に正当化される。

data/lecture/math/abstract-algebra/有限体の入口-講義.n.md md ff5949d

有限体の入口

finite field

有限体は、有限個の元しか持たない体である。有限なのに割り算ができるという点が重要であり、符号理論や暗号に現れる。

最初の例は、素数 p に対する

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

である。

1 何故素数が必要か

$\mathbb{Z}/n\mathbb{Z}$ が体になるには、0 でない剰余類が全て逆元を持つ必要がある。

$[a]$ が逆元を持つ条件は

$$\gcd(a, n) = 1$$

である。

もし $n = p$ が素数なら、$[a] \neq [0]$ であることは $p \nmid a$ を意味する。したがって $\gcd(a, p) = 1$ であり、逆元が存在する。

一方、n が合成数で $n = ab$、$1 < a, b < n$ と書けるなら、

$$[a][b] = [0]$$

だが $[a]$ も $[b]$ も 0 ではない。零因子があるので体ではない。

2 具体例：F_5

$\mathbb{F}_5 = \{[0], [1], [2], [3], [4]\}$ である。

[2] の逆元は [3] である。何故なら

$$[2][3] = [6] = [1]$$

だからである。

このように、有限体では有限個の表を使って足し算と掛け算を完全に記述できる。

3 素数冪の有限体

有限体の元の個数は、必ず

$$p^m$$

の形になる。ここで p は素数で、$m \geq 1$ である。

この事実の証明には、有限体をより詳しく調べる準備が必要である。このページでは、元の個数がどの形で現れるかという見通しとして使う。

$m = 1$ の場合が $\mathbb{F}_p$ である。$m > 1$ の有限体は、単に $\mathbb{Z}/p^m\mathbb{Z}$ ではない。実際、$\mathbb{Z}/4\mathbb{Z}$ には $[2]^2 = [0]$ という零因子があるので体ではない。

高次の有限体は、既約多項式で割った商環として構成される。

$$\mathbb{F}_p[x]/(f(x))$$

ここで $f(x)$ は $\mathbb{F}_p[x]$ の既約多項式である。

既約多項式とは、その係数の体の上で、定数でない二つの多項式の積に分解できない多項式である。この構成は見通しであり、このページの基本計算は $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を中心に行う。

4 何を変えて何を保存するか

有限体では、数の個数は有限になる。しかし、体としての加法、乗法、0 以外での割り算は保存される。有限性により、計算機で扱いやすく、暗号や誤り訂正に応用できる。

5　証明補足：有限整域は体である

有限な整域 R は体 である。
field

証明する。$a \in R$、$a \neq 0$ を取る。R が体であることを示すには、a の 乗法逆元 が存在することを示せばよい。

写像

$$\mu_a : R \to R, \qquad x \mapsto ax$$

を 考 える。$\mu_a(x) = \mu_a(y)$ とすると $ax = ay$ である。$a \neq 0$ で、R は整域なので消去法則より $x = y$ である。したがって μ_a は単射である。

R は有限集合なので、R から R への単射は全射である。よって $1 \in R$ に対して、ある $x \in R$ が存在して $ax = 1$ である。これは x が a の逆元であることを意味する。

有限性を使ったのは、単射から全射を 導 く箇所である。有限集合では、単射なら像の元数が 入力 の元数と同じになり、目標の 集合 も同じ大きさなので全ての元に届く。無限ではこの推論は一般には成り立たない。

6　演習 リンク

→ 基本演習 **整域・体・有限体** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/整域・体・有限体-基本演習/

7　まとめ

有限体は、有限個の元を持つ体である。$\mathbb{Z}/p\mathbb{Z}$ は素数 p のとき有限体になるが、合成数法では零因子が 生じるため体にならない。一般の有限体は素数冪個の元を持つ。

8 例：4 個の元を持つ有限体

$\mathbb{Z}/4\mathbb{Z}$ は体ではないが、4 個の元を持つ有限体は存在する。$\mathbb{F}_2[x]$ で

$$f(x) = x^2 + x + 1$$

を考える。この多項式は $\mathbb{F}_2$ 上で根を持たないので既約である。そこで

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$$

と定義する。$\alpha = [x]$ と書くと、関係式

$$\alpha^2 + \alpha + 1 = 0$$

から、標数 2 では

$$\alpha^2 = \alpha + 1$$

が成り立つ。したがって元は

$$0,\ 1,\ \alpha,\ \alpha + 1$$

の 4 個である。この例は、素数冪の有限体が $\mathbb{Z}/p^m\mathbb{Z}$ ではなく、既約多項式による商環として現れることを示している。

二次または三次の多項式では、根を持たないことから既約であることが分かる。また、標数 2 とは $1 + 1 = 0$ が成り立つという意味である。

data/lecture/math/abstract-algebra/準同型の基本-講義.n.md md 1e7b436

準同型の基本

homomorphism

準同型は、演算を保つ写像である。抽象代数では、対象そのものよりも、対象どうしを構造を壊さずに移す写像が重要になる。

線型代数で線型写像が加法とスカラー倍を保つように、抽象代数の準同型は群や環の演算を保つ。

→ 講義 線型写像と行列 lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/線型写像と行列-講義/

この類推は見通しであり、このページの定義と証明では、前に導入した群・環・写像だけを使う。

1 群準同型

group homomorphism

群 G, H の間の写像 $\varphi : G \to H$ が群準同型であるとは、

$$\varphi(ab) = \varphi(a)\varphi(b)$$

を満たすことである。

この条件から、単位元と逆元も保存される。

2 環準同型

ring homomorphism

環 R, S の間の写像 $\varphi : R \to S$ が環準同型であるとは、

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

を満たすことである。単位元を持つ環では、さらに

$$\varphi(1_R) = 1_S$$

を要求する流儀が多い。この教材では、単位元 (identity element) を保つ環準同型 (ring homomorphism) を 標準 とする。

3 核と像

kernel / image

準同型 (homomorphism) の核 (kernel) は、単位元 (identity element) または 0 に潰れる部分である。

群準同型 (group homomorphism) では

$$\ker \varphi = \{ g \in G \mid \varphi(g) = e_H \}$$

環準同型 (ring homomorphism) では

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0_S \}$$

である。

像 (image) は、実際に到達する元全体である。

$$\mathrm{Im}\, \varphi = \{ \varphi(x) \mid x \in \mathrm{domain} \}$$

4 何を変え、何を保存するか

準同型 (homomorphism) では、元の名前や表示は変わる。しかし、演算 (operation) してから写すことと、写してから演算 (operation) することが一致する。この意味で、準同型 (homomorphism) は構造 (structure) を保つ写像 (map) である。

同型 (isomorphism) は、可逆な準同型 (homomorphism) である。同型 (isomorphism) なら、構造 (structure) は完全に保存される。

5 演習リンク

→ 基本演習 **準同型と同型** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/準同型と同型-基本演習/

6 まとめ

準同型は、演算を保存する写像である。群準同型 は群の積を保ち、環準同型は加法と 乗法 を保つ。核は潰れる部分、像は到達する部分であり、 商構造 と準同型定理につながる。

7 例：評価写像は環準同型

体 F と $c \in F$ に対して、多項式環 $F[x]$ から F への写像

$$\mathrm{ev}_c : F[x] \to F, \qquad f(x) \mapsto f(c)$$

を評価写像という。これは環準同型である。なぜなら

$$\mathrm{ev}_c(f+g) = f(c) + g(c)$$

かつ

$$\mathrm{ev}_c(fg) = f(c)g(c)$$

が成り立つからである。

この写像の核は、c を根に持つ多項式全体である。つまり

$$\ker(\mathrm{ev}_c) = \{ f(x) \in F[x] \mid f(c) = 0 \}$$

である。核がイデアルになることは、準同型と 商環 が結びつく基本例である。

8 証明補足：環準同型の核はイデアルである

$\varphi : R \to S$ を環準同型とする。核を

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0 \}$$

で定義する。まず $\varphi(0_R) = 0_S$ なので、$0_R \in \ker\varphi$ であり、核は空ではない。$a, b \in \ker\varphi$ なら、

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$$

なので $a - b \in \ker\varphi$ である。また $r \in R$、$a \in \ker\varphi$ なら、

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0, \qquad \varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0$$

なので $ra, ar \in \ker\varphi$ である。したがって環準同型の核はイデアルである。

ideal

像 $\operatorname{Im}\varphi$ は、和・差・積について閉じている。さらに単位元を保つ流儀の環準同型では $\varphi(1_R) = 1_S$ なので、像は S の中で同じ演算を受け継ぐ部分環として扱える。

data/lecture/math/abstract-algebra/準同型定理の見取り図-講義.n.md md 2e84104

準同型定理の見取り図

homomorphism theorem

準同型定理の中心にある考えは単純である。準同型で同じ値に潰れる元を先に同一視すると、残った構造は像と同じになる。

この見方は、群、環、線型代数に共通している。

→ 講義 階数の基本 lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/階数の基本-講義/

線型代数は類似を示すための接続であり、このページの証明では群と環で導入した核・像・商だけを使う。

1 第一準同型定理の形

群準同型 $\varphi : G \to H$ に対して、

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

が成り立つ。

環準同型 $\varphi : R \to S$ に対しても、

$$R/\ker\varphi \cong \operatorname{Im}\varphi$$

が成り立つ。

式は同じ形である。違うのは、群では核が正規部分群であり、環では核がイデアルである点である。

2 何故そうなるか

写像 φ は、核の中の元を単位元または 0 に送る。したがって、核だけずれた元は同じ像を持つ。

群の場合、

$$g \ker \varphi$$

という剰余類を、

$$\varphi(g)$$

へ送る写像を考える。この写像は、代表元の選び方によらず定まる。もし $g \ker \varphi = g' \ker \varphi$ なら、$g^{-1}g' \in \ker \varphi$ なので $\varphi(g) = \varphi(g')$ である。

ここでは逆元を使っているため、群であることが必要である。

3 線型代数との対応

線型写像 $T : V \to W$ では、核は

$$\ker T = \{v \in V \mid T(v) = 0\}$$

であり、像は

$$\mathrm{Im}\, T = \{T(v) \mid v \in V\}$$

である。核方向を潰すと、残る自由度が像になる。この直感は、階数・退化・商空間の理解につながる。

→ 講義 **線型写像と行列** lecture math linear-algebra

https://study.bem130.com/lecture/math/linear-algebra/線型写像と行列-講義/

この対応は見通しであり、線型写像の定理を使って第一準同型定理を証明しているわけではない。

4 何が変わり、何が保存されるか

準同型定理では、核の中の違いを潰す。変わるのは元の識別の細かさである。保存されるのは、準同型によって実際に観測できる構造、つまり像である。

5 証明補足：第一同型定理の証明

$\varphi : G \to H$ を群準同型とする。第一同型定理 は

first isomorphism theorem

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

を主張する。

ここでは群の場合を証明する。環の場合も方針は同じで、正規部分群の代わりにイデアルを使う。

写像

$$\Phi : G/\ker\varphi \to \operatorname{Im}\varphi, \qquad g\ker\varphi \mapsto \varphi(g)$$

を定義する。まず well-defined であることを示す。$g\ker\varphi = g'\ker\varphi$ なら $g'^{-1}g \in \ker\varphi$ である。したがって

$$\varphi(g'^{-1}g) = e$$

であり、$\varphi(g')^{-1}\varphi(g) = e$ だから $\varphi(g) = \varphi(g')$ である。

つぎに Φ は準同型である。

$$\Phi((g\ker\varphi)(h\ker\varphi)) = \Phi(gh\ker\varphi) = \varphi(gh) = \varphi(g)\varphi(h)$$

である。全射は像の定義から 従う。単射は、$\Phi(g\ker\varphi) = e$ なら $\varphi(g) = e$、つまり $g \in \ker\varphi$ なので $g\ker\varphi = \ker\varphi$ となることから 従う。

よって Φ は同型であり、$G/\ker\varphi \cong \operatorname{Im}\varphi$ である。核で潰してから写すと、ちょうど像だけが残る、という直感がこの 証明 の内容である。

6 演習リンク

→ 基本演習 **準同型と同型** exercise math abstract-algebra

https://study.bem130.com/exercise/math/abstract-algebra/準同型と同型-基本演習/

7 まとめ

第一準同型定理は、「核で割ると像になる」という定理である。群、環、線型写像で同じ形が現れるため、抽象代数と線型代数を結ぶ重要な見取り図になる。