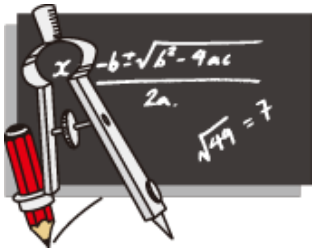
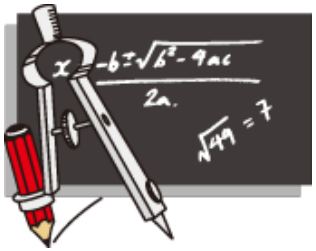


応用数学III
(12)群・環・体の定義

木村真一

講義のスケジュール



(1)　確率の基礎

(2)　確率変数と確率分布

(3)　いろいろな確率分布

(4)　多次元確率分布

(5)　大数の法則と中心極限定理

(6)　確率過程の基礎１

(7)　確率過程の基礎２

(8)　フーリエ解析

(9)　フーリエ変換の性質

(10)　相関解析

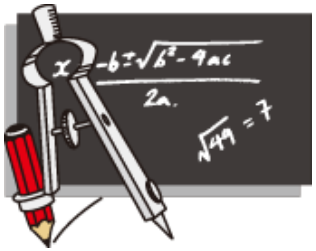
(11)　不確定信号の相関解析

(12)　群・環・体の定義

(13)　準同型写像

(14)　Nを法とする合同式

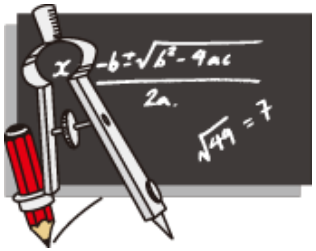
計算とは



- 私たちは加減乗除の四則演算普通に使っています。
- 足し算・かけ算は前後を入れ替えても答えは変わりませんが、引き算・割り算は前後を入れ替えると結果が変わってしまいます。
- ただ、引き算・割り算は、それぞれ足し算・かけ算の逆の計算です。ですから足し算・かけ算との関係で整理できそうです。
- 整数に対して足し算・引き算・かけ算をしても結果は整数です。ですが、割り算をすると結果が整数になるとは限りません。
- これに対して有理数、実数、複素数は四則演算いずれを行っても、結果はそれぞれ有理数、実数、複素数になります。

- 計算とそれを行う数の集合にはいくつかの法則がありそうです。
- ここでは数の集合と計算方法の法則について考えていきます。

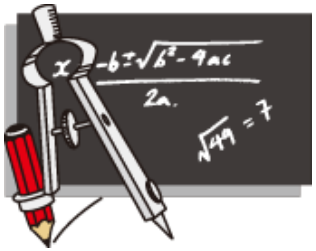
二項演算



- 二項演算：2個の元に対して一つの元を求める操作
  集合Sの上での写像

- 和や積は当然二項演算です
- 次のような一見計算とは関係なさそうな操作も全く同じように扱うことができます。
  - 正方行列のかけ算
  - Sをある集合Xの部分集合とするとき、$A, B \in S$　に対して
    $A \cap B, A \cup B$　　集合演算
  - Ｓを三次元線形空間とするとベクトルの外積

結合法則



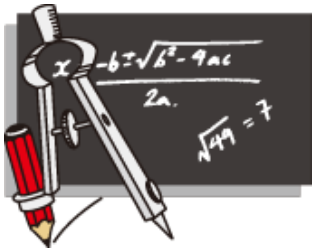
- 以下の関係が全ての $a,b,c \in S$ に対しても成り立つとき、演算 $\circ$ は結合法則を満たすと言います。

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- 普通の和や積の演算、正方行列のかけ算などは結合法則を満たします。
- 結合法則を満たすならば、演算の数が増えても、カッコのつけ方によらず答えは同じになります。

$$a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5 \circ \cdots \circ a_n$$

交換法則



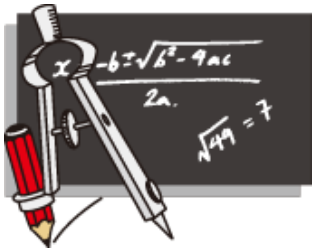
- 以下の関係が全ての $a,b,c \in S$ に対しても成り立つとき、演算 $\circ$ は結合法則を満たすと言います。

$$a \circ b = b \circ a$$

- 先の例で集合演算については交換法則が成り立ちますが、行列のかけ算、ベクトルの外積等は交換法則が成り立ちません。
- 結合法則と交換法則を満たすならば、演算の数が増えても、演算の順序を自由に変更できます。

$$a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5 \circ \cdots \circ a_n$$

単位元・逆元



- Sの元であって次の関係を満たすeを単位元と言います。

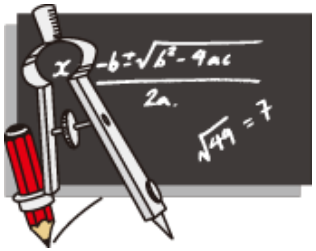
$$a \circ e = e \circ a = a$$

  - 実数に対する加算では0が単位元です。
  - 実数に対する乗算では1が単位元です。
- 単位元eが存在するとき、Sの元であって次の関係を満たすxを、aの逆元といいます。

$$a \circ x = x \circ a = e$$

  - 実数の加算の逆元を求める操作が減算です。
  - 実数の乗算の逆元を求める操作が除算です。

群の定義



- 集合G上に、次の性質を満たす二項演算 $\circ$ があるとき、Gは $\circ$ に関して群（group）であるといいます。

(G1) $\circ$ は結合法則を満たす。
即ち、どの $a,b,c \in G$ に対しても

$$(a \circ b) \circ c = a \circ (b \circ c)$$

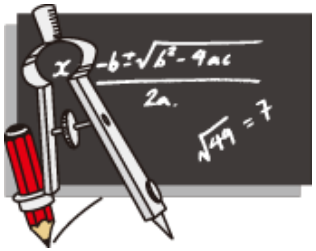
(G2)Gは単位元eを持つ

$$a \circ e = e \circ a = a$$

(G3)全ての $a \in G$ が逆元 a^{-1} を持つ。

$$a \circ a^{-1} = a^{-1} \circ a = e$$

群の種類



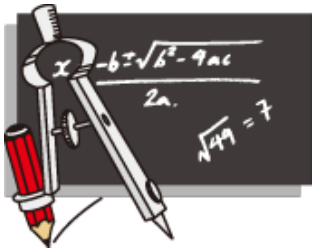
- 有限個の要素のみで構成される群

  有限群
- 無限個の要素を持つ群

  無限群
- 交換法則　$a \circ b = b \circ a$　が成り立つ群

  可換群またはアーベル群
  - 一般の群は交換法則が成り立つとは限りません。
  - アーベル群は”+”で表されることが多く、和群とも呼ばれます。

群の公理から導かれる性質

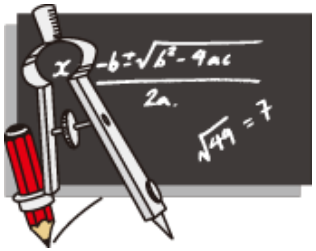


- 群の公理だけから導くことのできる性質があります。

- 単位元は一つしか存在しません
- 逆元は一つしか存在しません
- 与えられた $a,b \in G$ に対して $a \circ x = b, x \circ a = b$ を満たすxがただ一つ存在し、それぞれ $x = a^{-} \circ b, x = b \circ a^{-}$ である。

- それぞれ証明してみます。
- これらは群の種類によらず、群である限り必ず成り立ちます。

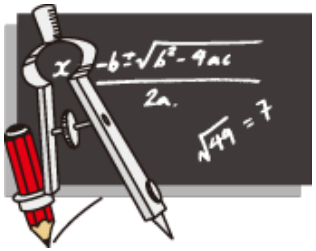
群の具体例



- 定義から明らかなように群は演算を対象にしています。
- 集合だけの性質ではありません。
- ですから、有理数、実数、複素数は、加法と乗法の2つの群を持ちます。

- $GL(n,\mathbf{R})$ を実数係数の行列式が０でないn×nの行列の集合としたとき、$GL(n,\mathbf{R})$ は行列の積について群になります。
- n×nの行列全体の集合が加法に関して群になります。
- 確認してみましょう。

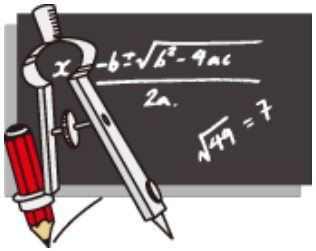
例題１



- 実数に対する演算として $a \circ b = a + b - 2$ と定義します。このときこの演算が群になることを示してください。
- また、単位元、逆元をそれぞれ求めてください。

- 単位元：２
- 逆元：4-a

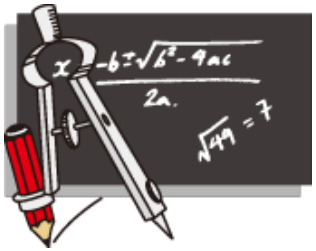
例題２



- 実数に対する演算として $a \circ b = ab - a - b + 2$ と定義します。このときこの演算は、そのままでは群ではないですが、ただ一つの元を除外すると群になります。その要素とは何ですか。
- また、その時の単位元、逆元をそれぞれ求めてください。

- 除外する元：１
- 単位元：２
- 逆元：$a/(a-1)$

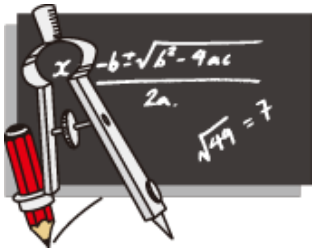
例題3



- $\mathbf{R}^2$ に対する演算として、$(a,b)\circ(c,d)=(c+ad,bd)$ を定義します。このとき集合 $G=\{(a,b)\in\mathbf{R}\,|\,b\neq 0\}$ がこの演算に関して群になることを示してください。
- また、その時の単位元、逆元をそれぞれ求めてください。

- 単位元：(0,1)
- 逆元：(-1/b,1/b)

環の定義



- 集合R上に、二つの二項演算、和”＋”と積”・”を定義し、次の性質を全て満たすときＲは環（ring）であると言います。

  （Ｒ１）加法に関してＲはアーベル群である。
  （加法の単位元を0、逆元を-aと書きます）

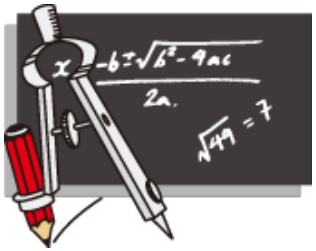
  （Ｒ２）乗法は結合法則を満たす。

  （Ｒ３）乗法の単位元が存在し、加法の単位元と異なる。

  （Ｒ４）分配法則が成り立つ。

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

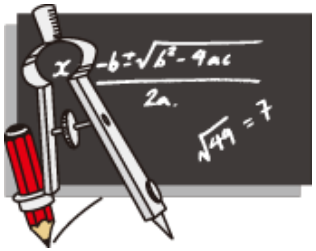
可換環



- 一般には乗法について交換法則が成り立つとは限りません。
  - 例）行列の積

- ここで交換法則 $ab = ba$ が常に成り立つ環のことを特に可換環と言います。
  - 可換環の例：
    - 整数、有理数、実数、複素数の演算
    - 多項式環
  - 可換でない環の例：
    - n×nの行列が行列の和と積に対してなす環

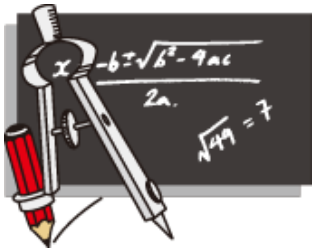
環の公理から導かれる性質



- 全ての　$a \in R$　に対して　$0a = 0$　です。

- まず、0=0+0です。
- R4より、a・0=a・(0+0)=a・0+a・0
- 両辺に- a・0を加えればa・0=0

体の定義



- ここまで来れば「体」はもうすぐそこです。

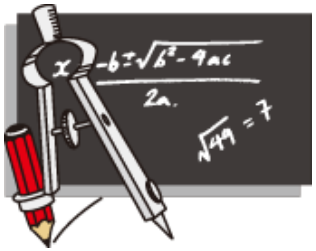
- Fが可換環であって、Fの0以外の元が、乗法に関する逆元をもつとき、Fは体（field）であるといいます。
  - 通常の加法・乗法について、有理数、実数、複素数は体です。
  - 平方数でないd に対して、以下の集合は体になります。

$$\mathbf{Q}\left[\sqrt{d}\right]=\left\{a+b\sqrt{d}\,\middle|\,a,b\in\mathbf{Q}\right\}$$

  - 似ていますが、以下の集合は体ではない可換環です。

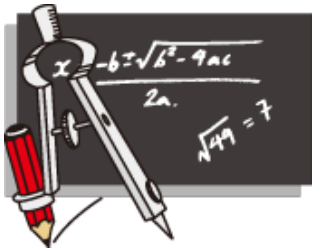
$$\mathbf{Z}\left[\sqrt{d}\right]=\left\{a+b\sqrt{d}\,\middle|\,a,b\in\mathbf{Z}\right\}$$

体の例



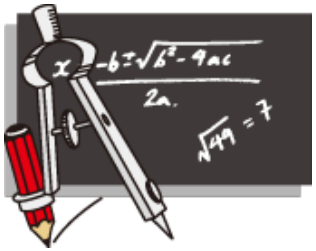
- $F=\{0,1\}$　二つの元を持つ集合とするとき以下のように定義するとFは体になります。
  - 0+0=0
  - 0+1=1
  - 1+1=0
  - 0・0=0・1=0
  - 1・1=1
- お気付きのように、これはコンピュータや情報処理においてとても大切な体です。

例題４



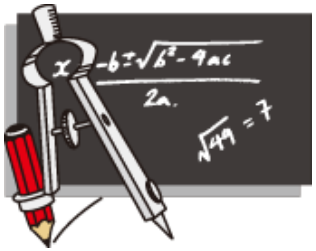
- ３つの元だけからなる集合 $G=\{a,b,e\}$ が、演算○について群になり、単位元がeだったとすると、ａ○ａ、ａ○ｂ、ｂ○ａ、ｂ○ｂ、はそれぞれ何になりますか。

例題５



- ４つの元からなる集合　$G=\{a,b,c,e\}$ が、演算○について群になり、単位元がeだったとします。このとき各演算の結果は２通り考えられます。
  １）　a○a= b○b= c○c=eになる場合、他の演算の結果はどうなるでしょう。
  ２）　a○a= bになる場合、他の演算の結果はどうなるでしょう。

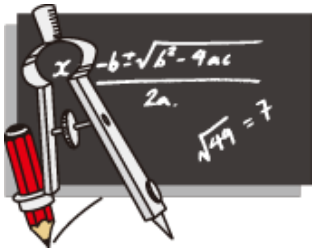
例題６



- $D = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a,b \in \mathbf{Q} \right\}$ とするとき、Dは行列の加法、

  乗法について、体を成すことを示してください

まとめ



- 二項演算
- 結合法則
- 交換法則
- 単位元・逆元
- 群
- 分配法則
- 環
- 体