離散数学及び演習
講義11　2016. 7. 7(木)

環(続き)
(教科書　pp.161-164)
群
(教科書　pp.168-170)

環(復習)

- 代数系$(R, +, \cdot)$は環である
  - 次の(1)～(7)が成り立つ.

(1) 任意の $x, y, z \in R$ に対して, $x+(y+z) = (x+y)+z$
(加法の結合則(associative law))

(2) $c \in R$ が存在して, 任意の $x \in R$ に対して, $x+c=c+x=x$
(加法の単位元の存在)

- c … 加法の単位元(unit element, identity element)(零元)

(3) 任意の $x \in R$ に対して, $y \in R$ が存在して, $x+y=y+x=c$
(加法の逆元の存在)

- $y=-x$ … x の加法の逆元(inverse element)

(4) 任意の $x, y \in R$ に対して, $x+y = y+x$
(加法の交換則(commutative law))

環(復習)(続き)

- 代数系$(R, +, \cdot)$は環である
  - 次の(1)～(7)が成り立つ.

(5) 任意の $x, y, z \in R$ に対して, $x\cdot(y\cdot z) = (x\cdot y)\cdot z$
(乗法の結合則(associative law))

(6) $e \in R$ が存在して, 任意の $x \in R$ に対して, $x\cdot e=e\cdot x=x$
(乗法の単位元の存在)

- e … 乗法の単位元(unit element, identity element)

(7) 任意の $x, y, z \in R$ に対して,
$x\cdot(y+z) = (x\cdot y)+(x\cdot z)$,
$(x+y)\cdot z = (x\cdot z)+(y\cdot z)$
(分配則(distributive law))

- 条件(1)～(7) … 環の公理(axiom)

可換環(復習)

- 代数系$(R, +, \cdot)$は可換環である
  - $(R, +, \cdot)$は環で, かつ, 次の(8)が成り立つ.

(8) 任意の $x, y \in R$ に対して, $x\cdot y = y\cdot x$
(乗法の交換則(commutative law))

体(field)

- 代数系$(F, +, \cdot, c, e)$は体(可換体)である
  - $(F, +, \cdot, c, e)$は環で, かつ, 次の(8), (9)が成り立つ.

(8) 任意の $x, y \in F$ に対して, $x\cdot y = y\cdot x$
(乗法の交換則(commutative law))

(9) 任意の $x \in F$ $(x \neq c)$に対して, $y \in F$ が存在して,
$x\cdot y = y\cdot x = e$
(乗法の逆元の存在)

- $y=x^{-1}$ … x の乗法の逆元(inverse element)
- x は可逆(invertible)である

- 代数系$(F, +, \cdot, c, e)$は斜体(skew field)である
  - $(F, +, \cdot, c, e)$は環で, かつ, 上の(9)が成り立つ.

体(続き)

例:

- $(\mathbf{Q}, +, \cdot, 0, 1)$ … 有理数体
- $(\mathbf{R}, +, \cdot, 0, 1)$ … 実数体
- $(\mathbf{C}, +, \cdot, 0, 1)$ … 複素数体
- $(\mathbf{Q}[i], +, \cdot, 0, 1)$ … Gauss の数体
  - $\mathbf{Q}[i] = \{ x+yi \mid x, y \in \mathbf{Q} \}$
    - 明らかに, $(\mathbf{Q}[i], +, \cdot, 0, 1)$は環である.
    - 明らかに, 乗法の交換則が成り立つ.
    - 任意の $x+yi \in \mathbf{Q}[i]$ $(x+yi \neq 0)$に対して,
$$\frac{1}{x+yi} = \frac{x}{x^2+y^2} + \frac{-y}{x^2+y^2} i \in \mathbf{Q}[i]$$
すなわち, 乗法の逆元が存在する.
- 整数環$(\mathbf{Z}, +, \cdot, 0, 1)$は体でない
  - 任意の $n \in \mathbf{Z}$ $(n \neq 0)$に対して, $1/n \in \mathbf{Z}$ であるとは限らない. +

定理

p が素数であるとき，かつそのときに限り，
$(\mathbf{Z}_p, +_p, \cdot_p)$ は体である．

- $\mathbf{Z}_p$（p は素数）
  … p 元体（field with p elements） $\mathbf{F}_p$

- $p \in \mathbf{Z}$ に対して，$\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$
  … $p \in \mathbf{Z}$ を法とする完全剰余系
  - $x +_p y = \mathrm{mod}(x+y, p)$
    $x \cdot_p y = \mathrm{mod}(x \cdot y, p)$
  - $(\mathbf{Z}_p, +_p, \cdot_p, 0, 1)$ は可換環．

- 任意の $x \in \mathbf{Z}_p$ $(x \neq 0)$ に対して，
  $y = x^{-1} \in \mathbf{Z}_p$ が存在して，$x \cdot y = y \cdot x = 1$
  （乗法の逆元の存在）
  - $\mathbf{Z}_3 = \{0, 1, 2\}$　　$1^{-1}=1,\ 2^{-1}=2$
  - $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$　　$1^{-1}=1,\ 2^{-1}=3,\ 3^{-1}=2,\ 4^{-1}=4$
  - $\mathbf{Z}_4 = \{0, 1, 2, 3\}$　　$1^{-1}=1,\ 2^{-1}$：存在しない，$3^{-1}=3$

乗算表（$p=3$）

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

乗算表（$p=4$）

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

7

証明

p が素数であるとき，かつそのときに限り，
$(\mathbf{Z}_p, +_p, \cdot_p)$ は体である．

- a)「p が素数ならば，$(\mathbf{Z}_p, +_p, \cdot_p)$ は体である」を示す．
- b)「$(\mathbf{Z}_p, +_p, \cdot_p)$ が体ならば，p は素数である」を示す．
- a) p は素数であると仮定して，乗法の逆元が存在することを示す．
  - 「任意の $k \in \mathbf{Z}_p$ $(k \neq 0)$ に対して，$y \in \mathbf{Z}_p$ が存在して，$k \cdot_p y = 1$」を示す．

---

a) p は素数であると仮定する．
$(\mathbf{Z}_p, +_p, \cdot_p)$ は可換環である．
また，任意の $k \in \mathbf{Z}_p$ $(k \neq 0)$ に対して，$1 \leq k < p$．
ゆえに，$\gcd(k, p) = 1$．
このとき，合同方程式 $ky \equiv 1 \pmod{p}$ の解 $y \in \mathbf{Z}_p$ が存在する．
すなわち，$y \in \mathbf{Z}_p$ が存在して，$k \cdot_p y = 1$．
乗法の逆元が存在するので，$(\mathbf{Z}_p, +_p, \cdot_p)$ は体である．

8

証明

p が素数であるとき，かつそのときに限り，
$(\mathbf{Z}_p, +_p, \cdot_p)$ は体である．

- b)「$(\mathbf{Z}_p, +_p, \cdot_p)$ が体ならば，p は素数である」を示す．
  - $(\mathbf{Z}_p, +_p, \cdot_p)$ が体であるとき，p は素数でないと仮定して，矛盾を導く．

---

b) $(\mathbf{Z}_p, +_p, \cdot_p)$ は体であると仮定する．
さらに，p は素数でないと仮定する．
このとき，p は合成数だから，
$k, s \in \mathbf{Z}$ $(1 < k, s < p)$ が存在して，$p = k \cdot s$．
$k \in \mathbf{Z}_p$ $(k \neq 0)$ だから，k の逆元 $y \in \mathbf{Z}_p$ が存在して，$k \cdot_p y = 1$．
ゆえに，$q \in \mathbf{Z}$ が存在して，$ky - 1 = q \cdot p = q \cdot k \cdot s$ だから，
$k(y - q \cdot s) = 1$．
$y - q \cdot s \in \mathbf{Z}$ だから，$1 < k$ に矛盾する．
ゆえに，p は素数である．

9

有限体（finite field）

- 体 $(F, +, \cdot)$ は有限体（Galois 体）である
  - F は有限集合である
  - $|F|$　… 有限体の位数（order）
  - 位数 q の有限体　… $GF(q)$

例：　p 元体 $\mathbf{F}_p$ は位数 p の有限体

- 符号理論，暗号理論への応用

E. Galois
（仏，1811-1832）

10

定理

体 $(F, +, \cdot)$ に対して，次の（1）～（4）が成り立つ．

（1）　加法の単位元は唯一である．
（2）　加法の逆元は唯一である．
（3）　乗法の単位元は唯一である．
（4）　乗法の逆元は唯一である．

- 体は環でもあるから，（1）～（3）が成り立つのは明らか．
- （4）は（2）と同様に示せる．

11

零因子（zero divisor）

- 環 $(R, +, \cdot, c, e)$ において，$x \in R$ は零因子である
  - $y \in R$ $(y \neq c)$ が存在して，$x \cdot y = y \cdot x = c$

例：
- 環 $(\mathbf{Z}_6, +_6, \cdot_6, 0, 1)$
  - $2 \in \mathbf{Z}_6$ は零因子
    - $3 \in \mathbf{Z}_6$ $(3 \neq 0)$ に対して，$2 \cdot_6 3 = 3 \cdot_6 2 = 0$
- 任意の環 $(R, +, \cdot, c, e)$
  - 零元 $c \in R$ は零因子
    - 任意の $y \in R$ $(y \neq c)$ に対して，$c \cdot y = y \cdot c = c$

12

整域（integral domain）

- 代数系$(R, +, \cdot, c, e)$は整域である
  - $(R, +, \cdot, c, e)$は可換環で，かつ，次の(10)が成り立つ．

(10)　任意の$x, y \in R$に対して，
$x \cdot y = c$ ならば，$x = c$ または $y = c$
（零元でない零因子の非存在）

(10')　任意の$x, y \in R$に対して，
$x \cdot y = c$ かつ $x \neq c$ ならば，$y = c$

整域（続き）

例：

- 整数環$(\mathbf{Z}, +, \cdot, 0, 1)$
  - 任意の$x, y \in \mathbf{Z}$に対して，$x \cdot y = 0$ ならば，$x = 0$ または $y = 0$
- 多項式環$(\mathbf{R}[x], +, \cdot, 0, 1)$
- p元体（$\mathbf{F}_p, +_p, \cdot_p, 0, 1$）($p$は素数)
  - 任意の$x, y \in \mathbf{F}_p$に対して，$x \cdot_p y = 0$ ならば，$x = 0$ または $y = 0$
  - 任意の$x, y \in \mathbf{F}_p$に対して，$x \cdot y \equiv 0 \pmod{p}$ ならば，
    $x \equiv 0 \pmod{p}$ または $y \equiv 0 \pmod{p}$．
  - 一般に，環（$\mathbf{Z}_p, +_p, \cdot_p, 0, 1$）は整域でない
    - 零元でない零因子が存在する．

例：行列環$M(n)$　$\begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix}\begin{bmatrix} 9 & -3 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

定理

可換環$(R, +, \cdot, c, e)$が整域であるとき，かつそのときに限り，次が成り立つ．
任意の$x, y, z \in R$に対して，
$x \cdot z = y \cdot z$ かつ $z \neq c$ ならば，$x = y$．
$z \cdot x = z \cdot y$ かつ $z \neq c$ ならば，$x = y$．
（消去則）

証明

可換環$(R, +, \cdot, c, e)$が整域であるとき，かつそのときに限り，次が成り立つ．
任意の$x, y, z \in R$に対して，$x \cdot z = y \cdot z$ かつ $z \neq c$ ならば，$x = y$．

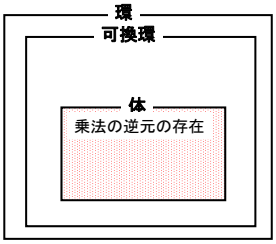
- a)「Rが整域であるとき，$x \cdot z = y \cdot z$ かつ $z \neq c$ ならば $x = y$」を示す．
- b)「$x \cdot z = y \cdot z$ かつ $z \neq c$ ならば $x = y$ であるとき，Rは整域である」を示す．

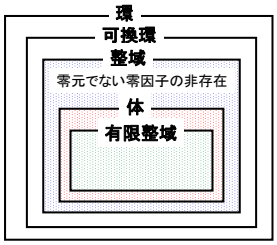
---

a)　Rは整域であると仮定する．
また，任意の$x, y, z \in R$に対して，$x \cdot z = y \cdot z$ かつ $z \neq c$と仮定する．
このとき，$x \cdot z + (-(y \cdot z)) = y \cdot z + (-(y \cdot z)) = c$．
分配則から，$(x + (-y)) \cdot z = c$．
Rは整域で，$z \neq c$だから，$x + (-y) = c$．
したがって，$x = -(-y) = y$．
b) 任意の$x, y, z \in R$に対して，$x \cdot z = y \cdot z$ かつ $z \neq c$ ならば $x = y$と仮定する．
ここで，$y = c$とおくと，$x \cdot z = c \cdot z$ かつ $z \neq c$ ならば，$x = c$．
ゆえに，$x \cdot z = c$ かつ $z \neq c$ ならば，$x = c$．
すなわち，Rは整域である．

定理

次の(1)，(2)が成り立つ．
(1)　体は整域である．
(2)　有限な整域は体である．





証明

(1)　体は整域である．

- 零元でない零因子は存在しないことを示す．
- 「任意の$x, y \in F$に対して，$x \cdot y = c$ かつ $x \neq c$ ならば，$y = c$」を示す．

$(F, +, \cdot, c, e)$を体とする．
任意の$x, y \in F$に対して，$x \cdot y = c$ かつ $x \neq c$とする．
このとき，Fは体だから，$x^{-1} \in F$が存在する．
ここで，$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot c = c$．
一方，$x^{-1} \cdot (x \cdot y) = (x^{-1} \cdot x) \cdot y = e \cdot y = y$．
したがって，$y = c$．

証明（続き）

(2)　有限な整域は体である.
- 乗法の逆元が存在することを示す.
  - 「任意の $x \in F\ (x \neq c)$ に対して，$y \in F$ が存在して，$x \cdot y = y \cdot x = e$」を示す.

$(F, +, \cdot, c, e)$を有限な整域とする.
まず，任意の $x \in F (x \neq c)$を考える.
関数 $f : F \to F$ を任意の $u \in F$ に対して $f(u) = x \cdot u$ と定義する.
任意の $u_1, u_2 \in F$ に対して，$f(u_1) = f(u_2)$ とする. このとき，$x \cdot u_1 = x \cdot u_2$.
ゆえに，$x \cdot u_1 + (-(x \cdot u_1)) = x \cdot u_2 + (-(x \cdot u_1))$だから，$c = x \cdot (u_2 + (-u_1))$.
$x \neq c$ で，F は整域だから，$u_2 + (-u_1) = c$.
ゆえに，$u_2 = u_1$ であり，f は単射である.
F は有限集合だから，f は全射でもある.
さらに，$F = \{u_1, u_2, \ldots, u_n\}$ とおくと，f は全単射だから，
$F = \{ f(u_1), f(u_2), \ldots, f(u_n) \} = \{ xu_1, xu_2, \ldots, xu_n \}$.
$e \in F$ だから，$u_i \in F$ が存在して，$xu_i = e$.
すなわち，任意の $x \in F (x \neq c)$に対して，乗法の逆元 u_i が存在する.

整域における整除関係

整域$(R, +, \cdot)$と $x, y \in R$ に対して，
- x は y の約元（factor）である
  y は x の倍元（multiple）である
  x は y を割り切る（divide）
  （y は x で割り切れる（divisible））

  … $x \mid y$
  - $q \in R$ が存在して，$y = q \cdot x$

公約元

整域$(R, +, \cdot)$と $x, y \in R$ に対して，
- $d \in R$ は x, y の公約元（common factor）である
  - $d \mid x$ かつ $d \mid y$.
- $d \in R$ は x, y の最大公約元（greatest common factor）である

  … $d = \gcd(x, y) = (x, y)$
  - d は x, y の公約元で，かつ，x, y の任意の公約元 d' に対して，$d' \mid d$ （d' は d の約元）.

定理

整域$(R, +, \cdot)$と任意の $a, b \in R$ に対して，
$x, y \in R$ が存在して，$a \cdot x + b \cdot y = \gcd(a, b)$.

素元（prime element）

整域$(R, +, \cdot, c, e)$に対して，
- $p \in R$ は素元である
  - p は次の(1)～(3)を満たす.
  (1)　p は可逆元でない（$p^{-1} \in R$ は存在しない）.
  (2)　$p \neq c$
  (3)　$x \cdot y \in R$ に対して，$p \mid x \cdot y$ ならば，$p \mid x$ または $p \mid y$.

例:
- 整域$(\mathbf{Z}, +, \cdot, 0, 1)$
  - 正の素元は素数.
- 整域$(\mathbf{R}[x], +, \cdot, 0, 1)$
  - 素元は既約多項式.

素元分解整域

- 代数系 $(R, +, \cdot, c, e)$ は素元分解整域（prime factorization domain）である
  - $(R, +, \cdot, c, e)$ は整域で，かつ，
    任意の $x \in R\ (x \neq c)$は，可逆元でなければ，
    有限個の素元 $p_1, p_2, \ldots, p_r$ に対して，
    $x = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素元の積の形）で表すことができる.

    - $x = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形

      … 素元分解（prime factorization）

定理

- 素元分解整域における素元分解の表現は，一意的である．
  - 素元分解整域　…　一意分解整域
    （unique factorization domain，UFD）
- 素元分解整域において，最大公約元は必ず存在する．

25

Euclid 域（Euclidean domain）

- 代数系$(R, +, \cdot, c, e)$は Euclid 域である
  - $(R, +, \cdot, c, e)$は整域で，かつ，
    関数 $v : R \to \mathbf{N}_0$ が存在して，次の(1)，(2)が成り立つ．
  - (1)　任意の $x, y \in R$（$x, y \neq c$）に対して，$v(x \cdot y) \geq v(x)$．
  - (2)　任意の $x, y \in R$（$y \neq c$）に対して，$q, r \in R$ が存在して，次の a)，b) が成り立つ．
    - a)　$x = q \cdot y + r$
    - b)　$r = c$ または　$v(r) < v(y)$
- 関数 v　…　R 上の付値（valuation）

例：

- $(\mathbf{Z}, +, \cdot, 0, 1)$　…　$v(x) = |x|$
- $(\mathbf{R}[x], +, \cdot, 0, 1)$　…　$v(P(x)) = \deg(P(x))$
- $(\mathbf{Z}[i], +, \cdot, 0, 1)$　…　$v(x + yi) = x^2 + y^2$

26

定理

- Euclid 域は素元分解整域である．
- Euclid 域$(R, +, \cdot, c, e)$と任意の $x, y, r, s \in R$に対して，$x = q \cdot y + r$ ならば，$\gcd(x, y) = \gcd(y, r)$．
  - Euclid の互除法により，最大公約元を求められる．

27

半群，モノイド

- 代数系 $(G, \cdot)$ は半群（semigroup）である
  - 次の(1)が成り立つ．
- (1)　任意の $x, y, z \in G$ に対して，$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  （結合則（associative law））
- 代数系 $(G, \cdot)$ はモノイド（monoid）（単位半群，unitary semigroup）である
  - $(G, \cdot)$ は半群で，かつ，次の(2)が成り立つ．
- (2)　$e \in G$ が存在して，任意の $x \in G$ に対して，$x \cdot e = e \cdot x = x$
  （単位元の存在）
  - e　…　単位元（unit element，identity element）

28

群（group）

- 代数系 $(G, \cdot)$ は群である
  - $(G, \cdot)$ はモノイドで，かつ，次の(3)が成り立つ．
- (3)　任意の $x \in G$ に対して，$y \in G$ が存在して，$x \cdot y = y \cdot x = e$
  （逆元の存在）
  - $y = x^{-1}$　…　逆元（inverse element）

29

群（続き）

- 代数系 G は群である
  - G 上に 1 つの演算が定義されている．
    （演算は G 上で閉じている）
  - 次の(1)～(3)（群の公理）が成り立つ．
- (1)　結合則
- (2)　単位元の存在
- (3)　逆元の存在

30

群（続き2）

例:

- モノイド
  - (**Z**, ＋, 0)
  - (**R**, ＋, 0)
  - (**Z**, ・, 1)
  - (**R**, ・, 1)
- 群
  - (**Z**, ＋, 0)
  - (**R**, ＋, 0)
  - (**R**－{0}, ・, 1)
  - (**Z**, ・, 1) はモノイドであるが，群ではない

31

可換群（commutative group）

- 代数系 $(G, \cdot)$ は可換群（Abel 群（Abelian group））である
  - $(G, \cdot)$ は群で，かつ，次の(4)が成り立つ.

(4) 任意の $x, y \in R$ に対して，$x \cdot y = y \cdot x$

（交換則（commutative law））

N. H. Abel
（ノルウェー，1802-1829）

32

乗法群，加法群

- 群 $(G, \cdot, e)$ … 乗法群（multicative group）
  - 単位元 e
  - $x \in G$ の逆元 x^{-1}
- 可換群 $(G, +, c)$ … 加法群（additive group）
  - 単位元 c（零元）
  - $x \in G$ の逆元 $-x$

33

群と環

- 環 $(R, +, \cdot)$ の公理

(1) 加法の結合則
(2) 加法の単位元の存在
(3) 加法の逆元の存在
(4) 加法の交換則
→ $(R, +)$ は加法群

(5) 乗法の結合則
(6) 乗法の単位元の存在
→ $(R, \cdot)$ はモノイド

(7) 分配則

34

群と体

- 体 $(F, +, \cdot)$ の公理

(1) 加法の結合則
(2) 加法の単位元の存在
(3) 加法の逆元の存在
(4) 加法の交換則
→ $(F, +)$ は加法群

(5) 乗法の結合則
(6) 乗法の単位元の存在
(9) 乗法の逆元の存在
(8) 乗法の交換則
→ $(F-\{c\}, \cdot)$ は可換乗法群

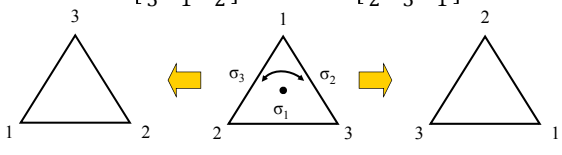
(7) 分配則

35

置換群（permutation group）

- 正三角形の回転における頂点の対応

$$\sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \qquad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$



$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

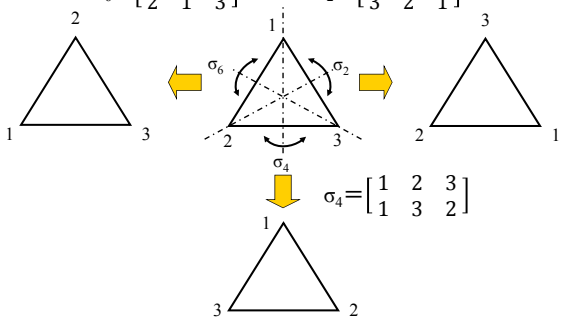
- σ_i … 頂点集合 $\{1, 2, 3\}$ 上の置換

36

置換群（続き）

- 正三角形の反転における頂点の対応

$$\sigma_6=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}\qquad \sigma_2=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$$

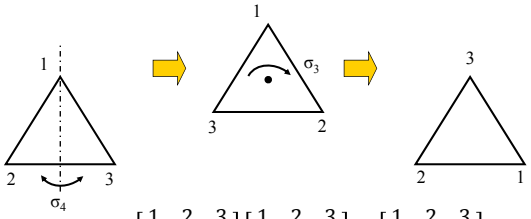


$$\sigma_4=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}$$

置換群（続き2）

- 正三角形の回転・反転の合成における頂点の対応

$$\sigma_4=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}\qquad \sigma_3=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$$

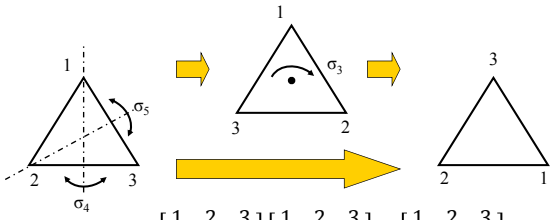


$$\sigma_3\cdot\sigma_4=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$$

置換群（続き3）

- 正三角形の回転・反転の合成における頂点の対応

$$\sigma_4=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}\qquad \sigma_3=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$$



$$\sigma_3\cdot\sigma_4=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}=\sigma_5$$

置換群（続き4）

- $S(3)=\left\{\begin{bmatrix}1&2&3\\i&j&k\end{bmatrix}\middle|\ \{i,j,k\}=\{1,2,3\}\right\}$
  $=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$
  - 集合 $\{1,2,3\}$ 上のすべての置換からなる集合
- $(S(3),\cdot)$ は群である　…　置換群
  - 演算・は $S(3)$ 上で閉じている
  - 演算・の結合則は成り立つ
  - 単位元 σ_1
  - 逆元
    $\sigma_1^{-1}=\sigma_1$, $\sigma_2^{-1}=\sigma_3$,
    $\sigma_3^{-1}=\sigma_2$, $\sigma_4^{-1}=\sigma_4$,
    $\sigma_5^{-1}=\sigma_5$, $\sigma_6^{-1}=\sigma_6$
  - 演算・は非可換
    $\sigma_3\cdot\sigma_4=\sigma_5$
    $\sigma_4\cdot\sigma_3=\sigma_6$
    $\sigma_3\cdot\sigma_4\neq\sigma_4\cdot\sigma_3$

乗積表（群表）

·	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_6	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

定理

次の(1)～(3)が成り立つ．
(1)　モノイドの単位元は唯一である．
(2)　群の単位元は唯一である．
(3)　群の逆元は唯一である．

- 環の単位元，逆元の唯一性と同様に示せる．

定理

代数系$(G,\cdot)$が次の(1)～(3)を満たすとき，かつそのときに限り，$(G,\cdot)$は群である．

(1)　任意の $x,y,z\in G$ に対して，$x\cdot(y\cdot z)=(x\cdot y)\cdot z$
（結合則(associative law)）

(2)　$e\in G$ が存在して，任意の $x\in G$ に対して，$x\cdot e=x$
（右単位元の存在）
- e　…　右単位元(right unit element, right identity element)

(3)　任意の $x\in G$ に対して，$y\in G$ が存在して，$x\cdot y=e$
（右逆元の存在）
- y　…　右逆元(right inverse element)

証明

代数系$(G, \cdot)$が次の(1)～(3)を満たすとき，かつそのときに限り，$(G, \cdot)$は群である．

(1)　任意の $x, y, z \in G$ に対して，$x \cdot (y \cdot z) = (x \cdot y) \cdot z$　(結合則)

(2)　$e \in G$ が存在して，任意の $x \in G$ に対して，$x \cdot e = x$　(右単位元の存在)

(3)　任意の $x \in G$ に対して，$y \in G$ が存在して，$x \cdot y = e$　(右逆元の存在)

- a)「$(G, \cdot)$が(1)～(3)を満たすならば，$(G, \cdot)$は群である」を示す．
- b)「$(G, \cdot)$は群ならば，$(G, \cdot)$は(1)～(3)を満たす」を示す．
  - 明らか．
- a)「$(G, \cdot)$に対して．群の公理が成り立つ」を示す．
  - a-1)「結合則が成り立つ」を示す．
  - a-2)「逆元が存在する」を示す．
  - a-3)「単位元が存在する」を示す．

---

a) 代数系$(G, \cdot)$が(1)～(3)を満たすと仮定する．

a-1) 明らかに，結合則は成り立つ．

証明(続き)

a)「代数系$(G, \cdot)$が(1)～(3)を満たすならば，$(G, \cdot)$は群である」を示す．

- a-2)「逆元が存在する」を示す．
- a-2)「左逆元が存在する」を示す．

---

a) 代数系$(G, \cdot)$が(1)～(3)を満たすと仮定する．

a-2) 右逆元の存在から，任意の $x \in G$ に対して，$y \in G$ が存在して，$x \cdot y = e$.

さらに，この y に対して，$z \in G$ が存在して，$y \cdot z = e$.

このとき，

$$\begin{aligned} y \cdot x &= y \cdot (x \cdot e) && \text{(右単位元)} \\ &= (y \cdot x) \cdot e && \text{(結合則)} \\ &= (y \cdot x) \cdot (y \cdot z) \\ &= ((y \cdot x) \cdot y) \cdot z && \text{(結合則)} \\ &= (y \cdot (x \cdot y)) \cdot z && \text{(結合則)} \\ &= (y \cdot e) \cdot z \\ &= y \cdot z && \text{(右単位元)} \\ &= e \end{aligned}$$

ゆえに，$x \cdot y = y \cdot x = e$ だから，y は x の逆元である．

証明(続き)

1)「代数系$(G, \cdot)$が(1)～(3)を満たすならば，$(G, \cdot)$は群である」を示す．

- a-3)「単位元が存在する」を示す．
- a-3)「左単位元が存在する」を示す．

---

a) 代数系$(G, \cdot)$が(1)～(3)を満たすと仮定する．

a-3) 逆元の存在から，任意の $x \in G$ に対して，$y \in G$ が存在して，$x \cdot y = y \cdot x = e$.

このとき，

$$\begin{aligned} e \cdot x &= (x \cdot y) \cdot x \\ &= x \cdot (y \cdot x) && \text{(結合則)} \\ &= x \cdot e \\ &= x && \text{(右単位元)} \end{aligned}$$

ゆえに，$x \cdot e = e \cdot x = x$ だから，e は単位元である．

系

代数系$(G, \cdot)$が次の(1)～(3)を満たすとき，かつそのときに限り，$(G, \cdot)$は群である．

(1)　任意の $x, y, z \in G$ に対して，$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(結合則(associative law))

(2)　$e \in G$ が存在して，任意の $x \in G$ に対して，$e \cdot x = x$
(左単位元の存在)

- e … 左単位元(left unit element, left identity element)

(3)　任意の $x \in G$ に対して，$y \in G$ が存在して，$y \cdot x = e$
(左逆元の存在)

- y … 左逆元(left inverse element)

まとめ

- 今日の講義
  - 環(続き)
  - 群
- 次回の講義
  - 部分系，準同型(教科書　pp.164-165, 170-173)
- 今回の演習
  - 環(続き)，群