離散数学及び演習
講義13　2016. 7.21（木）

商系
（教科書　pp.165-168 ）

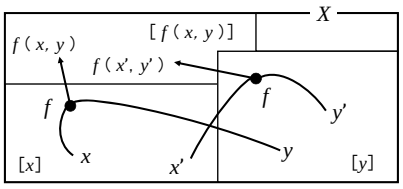
代数系の間の関係

- 代数系
  - 組$(X, f_1, f_2, \ldots, f_n)$
    - X は集合
    - $f_i : X^2 \to X$　（$i=1, 2, \ldots, n$）
- 代数系$(X, f_1, f_2, \ldots, f_n)$, $(Y, g_1, g_2, \ldots, g_n)$の間の関係
  - 部分系　　（前回講義）
  - 準同型，同型　（前回講義）
  - 商系

2

合同関係（congruent relation）

- 集合 X 上の2項演算 f と同値関係～ に対して，
  ～ は f と両立する（compatible）
  （～ は f に関して合同（congruent）である）
  - 任意の $x, x', y, y' \in X$ に対して，
    $x \sim x'$ かつ $y \sim y'$ ならば，$f(x, y) \sim f(x', y')$



3

合同関係（続き）

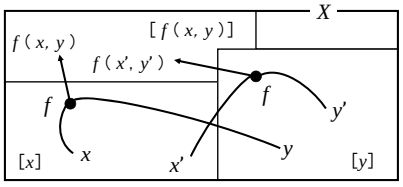
例：$p \in \mathbf{Z}$
　$\mathbf{Z}$ 上の同値関係$\equiv_p$，演算＋，・
- $\equiv_p = \{(m, n) \mid m \equiv n \pmod p\} \subseteq \mathbf{Z}^2$

- $\equiv_p$ は＋，・と両立する　（$\equiv_p$ は＋，・に関して合同である）
  - 任意の $m, m', n, n' \in \mathbf{Z}$ に対して，
    $m \equiv_p m'$ かつ $n \equiv_p n'$ ならば，
    $m+n \equiv_p m'+n'$，　$m \cdot n \equiv_p m' \cdot n'$

4

商系（quotient system）

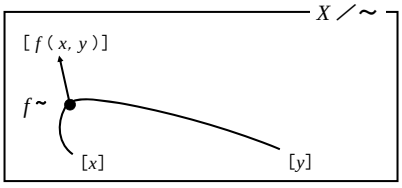
- 代数系(X, f)とf に関する X 上の合同関係～ に対する商系$(X/\sim, f^\sim)$
  - $X/\sim$　…　同値関係～による X の同値分割（商集合）
  - $f^\sim : (X/\sim)^2 \to X/\sim$
    任意の $[x], [y] \in X/\sim$ に対して，
    $f^\sim([x], [y]) = [f(x, y)]$



5

商系（quotient system）

- 代数系(X, f)とf に関する X 上の合同関係～ に対する商系$(X/\sim, f^\sim)$
  - $X/\sim$　…　同値関係～による X の同値分割（商集合）
  - $f^\sim : (X/\sim)^2 \to X/\sim$
    任意の $[x], [y] \in X/\sim$ に対して，
    $f^\sim([x], [y]) = [f(x, y)]$



6

商系（続き）

- $\mathbf{Z}$ 上の合同関係 $\equiv_3$
  - 同値分割 $\mathbf{Z}/\equiv_3 = \{[3k+r] \mid k \in \mathbf{Z},\ r=0,\ 1,\ 2\}$
  - $\equiv_3$ は演算＋，・に関して両立している
  - 商系（$\mathbf{Z}/\equiv_3$，＋，・）を定義できる
  - ただし，任意の $[m]$，$[n] \in \mathbf{Z}/\equiv_3$ に対して，
    - $[m]+[n]=[m+n]$，
    - $[m]\cdot[n]=[m\cdot n]$．

例：$4,\ 5 \in \mathbf{Z}$
- $[4]=[1]$，$[5]=[2]$
- $[4]+[5]=[4+5]=[9]=[0]$
  $[1]+[2]=[1+2]=[3]=[0]$
- $[4]\cdot[5]=[4\cdot5]=[20]=[2]$
  $[1]\cdot[2]=[1\cdot2]=[2]$

	$\mathbf{Z}$					
$[0]=[3]$	…	0	3	6	9	…
$[1]=[4]$	…	1	4	7	10	…
$[2]=[5]$	…	2	5	8	11	…

商系（続き）

- $\mathbf{Z}$ 上の合同関係 $\equiv_3$
  - 同値分割 $\mathbf{Z}/\equiv_3 = \{[3k+r] \mid k \in \mathbf{Z},\ r=0,\ 1,\ 2\}$
  - $\equiv_3$ は演算＋，・に関して両立している
  - 商系（$\mathbf{Z}/\equiv_3$，＋，・）を定義できる
  - ただし，任意の $[m]$，$[n] \in \mathbf{Z}/\equiv_3$ に対して，
    - $[m]+[n]=[m+n]$，
    - $[m]\cdot[n]=[m\cdot n]$．

例：$4,\ 5 \in \mathbf{Z}$
- $[4]=[1]$，$[5]=[2]$
- $[4]+[5]=[4+5]=[9]=[0]$
  $[1]+[2]=[1+2]=[3]=[0]$
- $[4]\cdot[5]=[4\cdot5]=[20]=[2]$
  $[1]\cdot[2]=[1\cdot2]=[2]$

$\mathbf{Z}/\equiv_3$
$[0]\,(=[3]=[6]=\ldots)$
$[1]\,(=[4]=[7]=\ldots)$
$[2]\,(=[5]=[8]=\ldots)$

商系（続き3）

- 商系（$\mathbf{Z}/\equiv_3$，＋，・）上の演算
  - 任意の $[m]$，$[n] \in \mathbf{Z}/\equiv_3$ に対して，
    - $[m]+[n]=[m+n]$，
    - $[m]\cdot[n]=[m\cdot n]$．

加算表

＋	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

乗算表

・	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

定理

$p \in \mathbf{Z}$ に対して，商系（$\mathbf{Z}/\equiv_p$，＋，・）は可換環である．
ただし，任意の $[m]$，$[n] \in \mathbf{Z}/\equiv_p$ に対して，
- $[m]+[n]=[m+n]$，
- $[m]\cdot[n]=[m\cdot n]$．

- （$\mathbf{Z}/\equiv_p$，＋，・）
  … $p \in \mathbf{Z}$ を法とする剰余環（residue class ring）

証明

$p \in \mathbf{Z}$ に対して，商系（$\mathbf{Z}/\equiv_p$，＋，・）は可換環である．
- 「（$\mathbf{Z}/\equiv_p$，＋，・）は可換環の公理を満たす」を示す．

1）任意の $[m]$，$[n]$，$[k] \in \mathbf{Z}/\equiv_p$ に対して，

$$\begin{aligned}([m]+[n])+[k] &= [m+n]+[k]\\ &= [(m+n)+k]\\ &= [m+(n+k)]\\ &= [m]+[n+k]\\ &= [m]+([n]+[k]).\end{aligned}$$

ゆえに，加法の結合則は成り立つ．

証明（続き）

$p \in \mathbf{Z}$ に対して，商系（$\mathbf{Z}/\equiv_p$，＋，・）は可換環である．
- 「（$\mathbf{Z}/\equiv_p$，＋，・）は可換環の公理を満たす」を示す．

2）$[0] \in \mathbf{Z}/\equiv_p$ を考えると，任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して，
$[m]+[0]=[m+0]=[m]$，$[0]+[m]=[0+m]=[m]$だから，
$[m]+[0]=[0]+[m]=[m]$．
すなわち，$[0]$は加法の単位元である．

3）任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して，$[-m] \in \mathbf{Z}/\equiv_p$を考えると，
$[m]+[-m]=[m+(-m)]=[0]$，
$[-m]+[m]=[(-m)+m]=[0]$
だから，
$[m]+[-m]=[-m]+[m]=[0]$．
すなわち，$[m]$に対して $[-m]$は加法の逆元である．

証明（続き2）

$p \in \mathbf{Z}$ に対して，商系（$\mathbf{Z}/\equiv_p$，＋，・）は可換環である．

- 「（$\mathbf{Z}/\equiv_p$，＋，・）は可換環の公理を満たす」を示す．

---

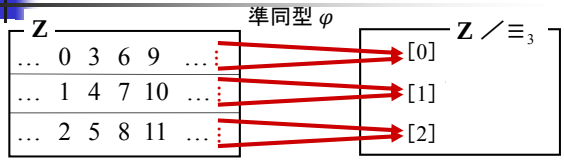
4) 任意の $[m]$，$[n] \in \mathbf{Z}/\equiv_p$ に対して，
$[m]+[n] = [m+n]$
$= [n+m]$
$= [n]+[m]$
ゆえに，加法の交換則は成り立つ．
5) 乗法の結合則は成り立つ．
6) $[1] \in \mathbf{Z}/\equiv_p$ を考えると，任意の $[m] \in \mathbf{Z}/\equiv_p$ に対して，
$[m]\cdot[1]=[m\cdot 1]=[m]$，$[1]\cdot[m]=[1\cdot m]=[m]$ だから，
$[m]\cdot[1]=[1]\cdot[m]=[m]$．
すなわち，$[1]$ は乗法の単位元である．
7) 分配則は成り立つ．
8) 乗法の交換則は成り立つ．
以上から，（$\mathbf{Z}/\equiv_p$，＋，・）は可換環である．

定理

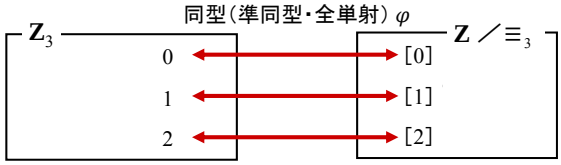
次の(1)，(2)が成り立つ．
(1)　$p \in \mathbf{Z}$ に対して，
剰余環（$\mathbf{Z}/\equiv_p$，＋，・）は整数環（$\mathbf{Z}$，＋，・）に準同型である．
(2)　$p \in \mathbf{N}$ に対して，
剰余環（$\mathbf{Z}/\equiv_p$，＋，・）と環（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は同型である．
ただし，$\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$（完全代表系）．

- $[m] \in \mathbf{Z}/\equiv_p$ と $m \in \mathbf{Z}_p$ を同一視すれば，
（$\mathbf{Z}/\equiv_p$，＋，・）と（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は「同じもの」．

整数環・完全代表系と剰余環



任意の $n \in \mathbf{Z}$ に対して，$\varphi(n) = [n]$．



任意の $n \in \mathbf{Z}_3$ に対して，$\varphi(n) = [n]$．

証明

(1)　$p \in \mathbf{Z}$ に対して，（$\mathbf{Z}/\equiv_p$，＋，・）は（$\mathbf{Z}$，＋，・）に準同型である．

- 「準同型 $\varphi: \mathbf{Z} \to \mathbf{Z}/\equiv_p$ が存在する」を示す．

$\varphi: \mathbf{Z} \to \mathbf{Z}/\equiv_p$ を次のように定義する．
任意の $n \in \mathbf{Z}$ に対して，$\varphi(n) = [n]$．
このとき，任意の m，$n \in \mathbf{Z}$ に対して，
$\varphi(m+n) = [m+n] = [m]+[n] = \varphi(m)+\varphi(n)$，
$\varphi(m\cdot n) = [m\cdot n] = [m]\cdot[n] = \varphi(m)\cdot\varphi(n)$．
ゆえに，φ は準同型である．

証明（続き）

(2)　$p \in \mathbf{N}$ に対して，（$\mathbf{Z}/\equiv_p$，＋，・）と（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は同型である．

- a) 「準同型 $\varphi: \mathbf{Z}_p \to \mathbf{Z}/\equiv_p$ が存在する」を示す．
- b) 「φ は全単射である」を示す．

---

a) $\varphi: \mathbf{Z}_p \to \mathbf{Z}/\equiv_p$ を次のように定義する．
任意の $n \in \mathbf{Z}_p$ に対して，$\varphi(n) = [n]$．
(1)と同様に，φ は準同型である．
b-1) 任意の m，$n \in \mathbf{Z}_p$ に対して，$\varphi(m) = \varphi(n)$ とする．
このとき，$[m] = [n]$．すなわち，$m \equiv_p n$．
$0 \le m, n < p$ だから，$m = n$．ゆえに，φ は単射である．
b-2) 任意の $n \in \mathbf{Z}$ に対して，q，$r \in \mathbf{Z}$ が存在して，$n = qp + r$ $(0 \le r < |p|)$．
このとき，$n \equiv_p r$．
ゆえに，任意の $[n] \in \mathbf{Z}/\equiv_p$ に対して，$r \in \mathbf{Z}_p$ が存在して，
$\varphi(r) = [r] = [n]$．
ゆえに，φ は全射である．
以上から，（$\mathbf{Z}/\equiv_p$，＋，・）と（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は同型である．

商系（quotient system）（再掲）

- 代数系（X，f）と f に関する X 上の合同関係～ に対する商系（$X/\sim$，$f^\sim$）
  - $X/\sim$　…　同値関係～による X の同値分割（商集合）
  - $f^\sim: (X/\sim)^2 \to X/\sim$
    任意の $[x]$，$[y] \in X/\sim$ に対して，
    $f^\sim([x], [y]) = [f(x, y)]$
- 集合 X 上の2項演算 f と同値関係～ に対して，
～ は f と両立する（compatible）
（～ は f に関して合同（congruent）である）
  - 任意の x，x'，y，$y' \in X$ に対して，
    $x \sim x'$ かつ $y \sim y'$ ならば，$f(x, y) \sim f(x', y')$

商系における合同関係

- 代数系$(X/\sim, f^{\sim})$
  - X 上の同値関係$\sim$は f に関して両立していないとする
    - X 上の同値関係$\sim$は f に関する合同関係ではないとする
  - 任意の $[x], [y] \in X/\sim$ に対して，
    $f^{\sim}([x], [y]) = [f(x, y)]$とする．
  - このとき，矛盾が生じる．
    - 商系の定義の際には，同値関係$\sim$が f と両立していることが必要．

同値関係$\sim$は f に関して両立していないので，ある $x, x', y, y' \in \mathbf{Z}$ に対して，
$x \sim x'$かつ $y \sim y'$ であるが，$f(x, y) \sim f(x', y')$でない．
ところで，$f^{\sim}([x], [y]) = [f(x, y)]$．
また，$x \sim x'$かつ $y \sim y'$ だから，$[x] = [x']$かつ $[y] = [y']$．
ゆえに，$f^{\sim}([x], [y]) = f^{\sim}([x'], [y']) = [f(x', y')]$．
すなわち，$[f(x, y)] = [f(x', y')]$だから，$f(x, y) \sim f(x', y')$．
これは矛盾．

[参考]ベクトル空間

（全学共通科目・線形代数Ⅱ　1年後期）

ベクトル空間

集合 V はベクトル空間（線形空間）である．

- V は次の I, II を満たす．

I（ベクトル加法の公理）
任意の $\boldsymbol{a}, \boldsymbol{b} \in V$ に対して，$\boldsymbol{a}+\boldsymbol{b} \in V$ が定義され，
次の(1)～(4)を満たす．

(1) $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c} = \boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$　（結合則）
(2) $\boldsymbol{0} \in V$ が存在して，任意の$\boldsymbol{a} \in V$ に対して，
$\boldsymbol{a}+\boldsymbol{0} = \boldsymbol{0}+\boldsymbol{a} = \boldsymbol{a}$　（単位元の存在）
(3) 任意の$\boldsymbol{a} \in V$ に対して，$-\boldsymbol{a} \in V$ が存在して，
$\boldsymbol{a}+(-\boldsymbol{a}) = (-\boldsymbol{a})+\boldsymbol{a} = \boldsymbol{0}$　（逆元の存在）
(4) $\boldsymbol{a}+\boldsymbol{b} = \boldsymbol{b}+\boldsymbol{a}$　（交換則）

ベクトル空間（続き）

集合 V はベクトル空間（線形空間）である．

- V は次の I, II を満たす．

II（スカラー乗法の公理）
任意の $\boldsymbol{a} \in V$ と任意の $k \in \mathbf{R}$ に対して，$k\boldsymbol{a} \in V$ が定義され，
次の(1)～(4)を満たす．

(1) $h(k\boldsymbol{a}) = (hk)\boldsymbol{a}$　（結合則）
(2) $(h+k)\boldsymbol{a} = h\boldsymbol{a}+k\boldsymbol{a}$　（分配則）
(3) $k(\boldsymbol{a}+\boldsymbol{b}) = k\boldsymbol{a}+k\boldsymbol{b}$　（分配則）
(4) $1\boldsymbol{a} = \boldsymbol{a}$

ベクトル空間の例

- すべての n 次元数ベクトルからなる集合
  $\mathbf{R}_n = \{ {}^t(a_0, a_1, \ldots, a_n) \mid a_i \in \mathbf{R}\ (i = 1, 2, \ldots, n) \}$
- すべての $m \times n$ 行列からなる集合$M(m, n)$
- すべての 1 変数実係数多項式からなる集合
  $\mathbf{R}[x] = \{ a_n x^n + \ldots + a_1 x + a_0 \mid a_i \in \mathbf{R}\ (i = 0, 1, \ldots, n) \}$
- すべての実数列からなる集合
- 閉区間$[a, b]$上のすべての連続関数からなる集合
- 同次連立1次方程式 $\mathbf{A}x = \mathbf{0}$ のすべての解からなる集合
- 2階線形微分方程式 $f''(x) + pf'(x) + qf(x) = 0\ (p, q \in \mathbf{R})$ のすべての解からなる集合

ベクトル空間（続き2）

集合 V はベクトル空間（線形空間）である．

- V は次の I, II を満たす．

I（ベクトル加法の公理）
任意の $\boldsymbol{a}, \boldsymbol{b} \in V$ に対して，$\boldsymbol{a}+\boldsymbol{b} \in V$ が定義され，
次の(1)～(4)を満たす．

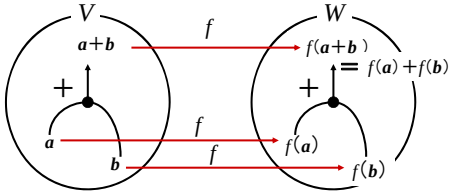
(1) $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c} = \boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$　（結合則）
(2) 任意の$\boldsymbol{a} \in V$ に対して，$\boldsymbol{0} \in V$ が存在して，
$\boldsymbol{a}+\boldsymbol{0} = \boldsymbol{0}+\boldsymbol{a} = \boldsymbol{a}$　（単位元の存在）
(3) 任意の$\boldsymbol{a} \in V$ に対して，$-\boldsymbol{a} \in V$ が存在して，
$\boldsymbol{a}+(-\boldsymbol{a}) = (-\boldsymbol{a})+\boldsymbol{a} = \boldsymbol{0}$　（逆元の存在）
(4) $\boldsymbol{a}+\boldsymbol{b} = \boldsymbol{b}+\boldsymbol{a}$　（交換則）

ベクトル空間$(V, +, \boldsymbol{0})$は可換群である

線形写像

ベクトル空間 V，W に対して，写像 $f: V \to W$ は線形写像である

- 任意の $\boldsymbol{a}, \boldsymbol{b} \in V$ と任意の $k \in \mathbf{R}$ に対して，次の(1)，(2)を満たす．
  - (1) $f(\boldsymbol{a}+\boldsymbol{b}) = f(\boldsymbol{a}) + f(\boldsymbol{b})$
  - (2) $f(k\boldsymbol{a}) = k f(\boldsymbol{a})$



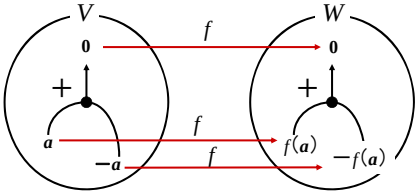
f は群準同型である

線形写像の性質

ベクトル空間 V，W と線形写像 $f: V \to W$ に対して，次の(1)，(2)が成り立つ．

(1) $f(\mathbf{0}) = \mathbf{0}$

(2) $f(-\boldsymbol{a}) = -f(\boldsymbol{a})$



群準同型写像は単位元と逆元を保存する．

まとめ

- 今日の講義
  - 商系
- 期末試験(7／28　2 限)
  - 試験範囲:　講義1～13(全体)
  - 持込み不可
  - 教室:　143･144(演習時と同じ)
  - 演習問題解答例(pdf 版)
    - http://www.kl.i.is.nagoya-u.ac.jp/~toyama/lecture/risan16/
- 今回の演習
  - 商系

成績評価(再掲)

- 中間試験 ― 約30%
  - 各自の得点は NUCT (https://ct.nagoya-u.ac.jp/)で確認可能
- 期末試験 ― 約40%
- 小テスト
- 演習解答
- 演習板書

　} 約30%

- 評価区分
  - 2011年度以降入学者
    S:100～90, A: 89～ 80, B: 79～70, C:69～60, F:59～0
  - 2010年度以前入学者
    優:100～80, 良:79～70, 可:69～60, 不可: 59～0
  - 期末試験を欠席した場合は,「欠席」とする.
- 不合格の場合
  - 来年度も同じクラスで受講

講義の目的(再掲)

- 離散的対象に関する知識の習得
  様々な分野に対する基礎的知識の習得
  - 集合論
  - 整数論
  - 代数系
- 概念を客観的かつ論理的に表現，論証するための手法･技術の習得
  - 数学的表現
  - 論証技術
- 講義目的の達成度＝成績評価基準