幾何学入門第４回
群というアイデアで遊ぶ

名城大学理工学部情報工学科
山本修身

集合に付加される色々な構造

- 位相空間＝集合＋開集合族
- 距離空間＝集合＋距離
- 代数構造＝集合＋演算
- 順序構造＝集合＋順序

たとえば，整数の集合はいくつかの側面がある

集合に色々な構造を付加することによって多様な現象を表現することができる

色々な代数構造

なかなか特定の性質が
言いづらい　単純

- 半群 (semigroup) ⇒ 正の整数の全体
- モノイド (monoid) ⇒ 文字列の集合（空列を含む） $\sum^*$
- 群 (group) ⇒ ベクトル空間，行列の積の集合

- 環 (ring) ⇒ 多項式，整数の集合
- 体 (field) ⇒ 実数，有理数の集合，有理式の集合

複雑

色々なことが言える．現実の
現象に適用しづらい

群はポピュラーな構造としては最も単純

- ある程度の性質が成り立つ代数構造の中で最も単純なものが**群 (group)** である.

- 我々が知っている多くの対象が群として捉えることができる.
- 例：整数, 分数などの数. ベクトル空間. 行列の積の空間. 符号の空間

群とは何か（定義）

- **群 (group)** は集合 X と X の任意の2つの元 a, b の間に定義された演算 * によって a * b が定義される世界である．ただし，演算はつぎの性質を満たす
  - a * b ∈ X（閉じていること）

- (a * b) * c = a * (b * c)　（結合則）
- a * e = e * a = a となる元 e が存在する（単位元の存在）．
- 任意のaについてa * b = b * a = e となる b = a^{-1}が存在する （逆元の存在）．

群の例（整数の足し算，引き算）

- 整数の集合をZと書く．Zは足し算に関して群をなす．
- なぜならば，
  - (k + m) + n = k + (m + n)
  - m + 0 = 0 + m = m
  - m + (-m) = (-m) + m = 0

群でない例（整数のかけ算）

- 足し算に関して整数は群であるが，かけ算に関しては群でない．
  - k * (m * n) = (k * m) * n
  - l * m = m * l = m
  - m * n = 1 となる nが任意のmについて存在しない！
  - そこで，1/m という数を考えると分数になる．分数まで考えると，群になる．積について群になるように要素を増やしたものが**有理数の集合**である．

体

整数の符号について考える
（符号だけでも群になる）

- 整数の符号だけに着目する

（＋）×（＋）＝（＋）
（－）×（＋）＝（－）
（＋）×（－）＝（－）
（－）×（－）＝（＋）

実際の演算

×	＋	－
＋	＋	－
－	－	＋

演算表

単位元

X = {(+), (–)}　←これは群となる

整数は積について群をなさないが...

- 整数は積について群をなさない.

しかし ↓

Y = { I, -I }　は積について群をなす

単位元

×	1	−1
1	1	−1
−1	−1	1

群の単位元は１つしかない！

- １つの群に２つ以上の単位元は存在しない.
- もし，２つあったとすると...

$$e_1 e_2 = e_2 = e_1$$

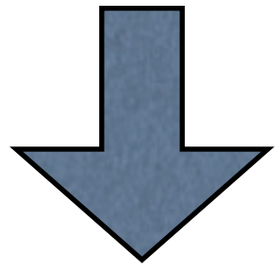
となり，同じになってしまう.

右逆元と左逆元は一致する

- 左側からかけた逆元（左逆元）と右からかけた逆元は同じものである.

$$a_1^{-1}a = e$$

$$aa_2^{-1} = e$$



$$a_1^{-1} = a_1^{-1}e = a_1^{-1}aa_2^{-1} = ea_2^{-1} = a_2^{-1}$$

可換でない群の例

- U = {e, s, t, x, y, z}

3次の対称群

	e	s	t	x	y	z
e	e	s	t	x	y	z
s	s	t	e	y	z	x
t	t	e	s	z	x	y
x	x	z	y	e	t	s
y	y	x	z	s	e	t
z	z	y	x	t	s	e

これは群に
なっている

$$(sx)y = zy = t$$

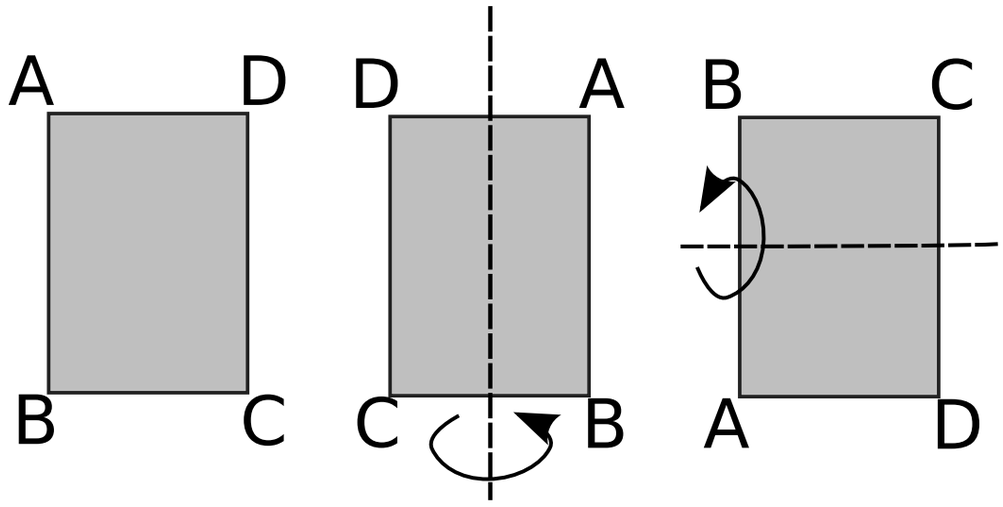
$$s(xy) = ss = t$$

確認するのは大変

種明かしはあとから

可換な群の例

- クラインの4元群



e τ σ

表 6.1: クラインの四元群の演算表

	e	τ	σ	$\tau\sigma$
e	e	τ	σ	$\tau\sigma$
τ	τ	e	$\tau\sigma$	σ
σ	σ	$\tau\sigma$	e	τ
$\tau\sigma$	$\tau\sigma$	σ	τ	e

F. Klein
(1849-1925)

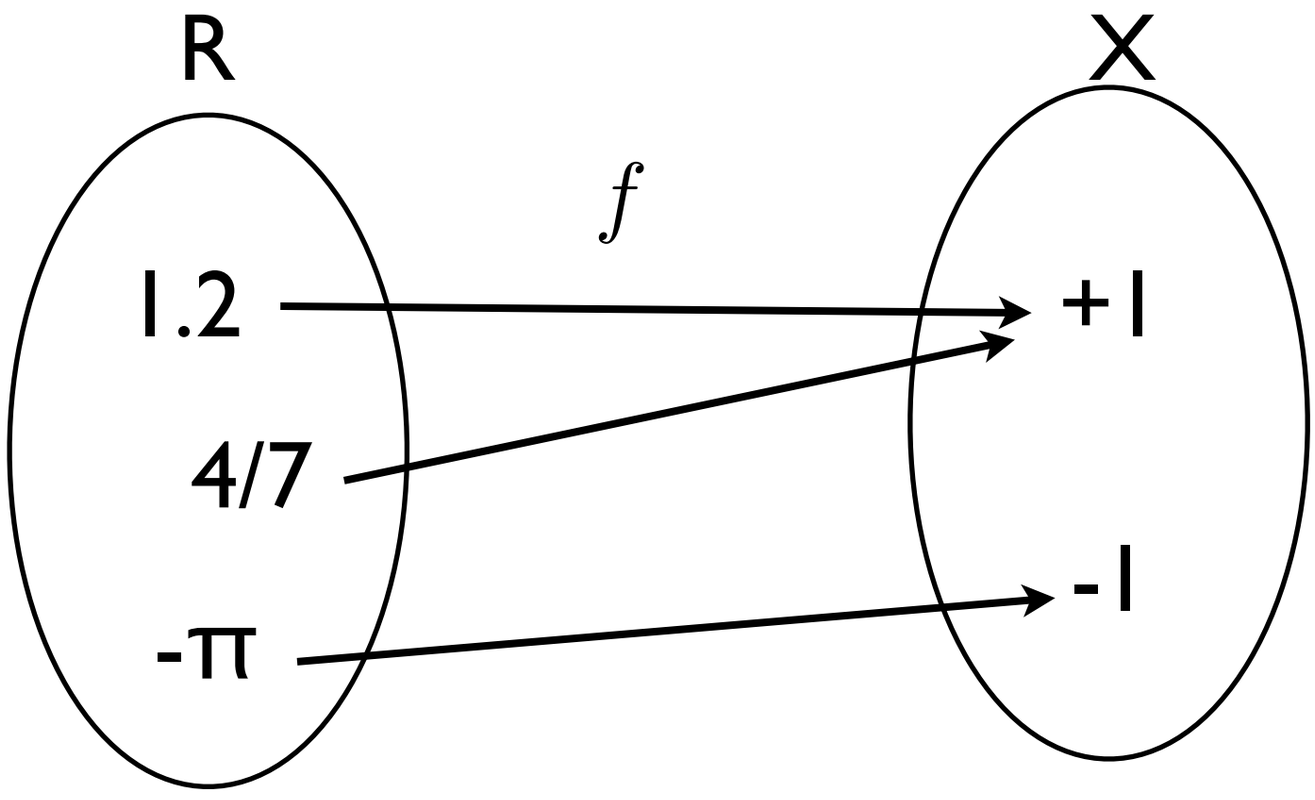
$$G = \{e, \tau, \sigma, \tau\sigma\}$$

$$\tau\sigma = \sigma\tau$$

$$\tau^2 = e, \quad \sigma^2 = e$$

実数から符号の世界へ

- 実数の集合（０以外）は積について群をなす.

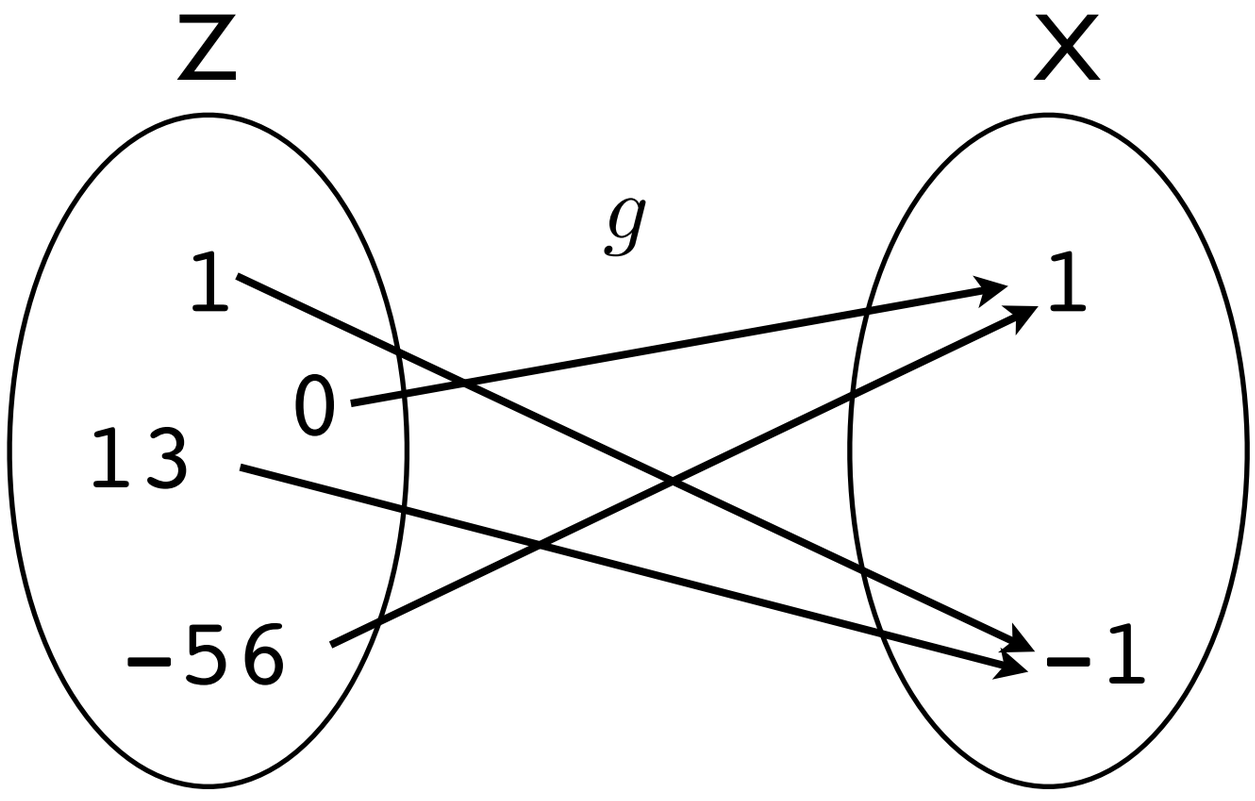


$$f(x \times y) = f(x) \times f(y)$$ 準同形

RもXも群の構造をもっている

2で割ったあまりを考える

- 今度は整数の足し算の世界を考える.



２で割り切れたら１
割り切れなければ−１

Y = {1, −1}

これも準同形

$$g(x+y) = g(x)g(y)$$

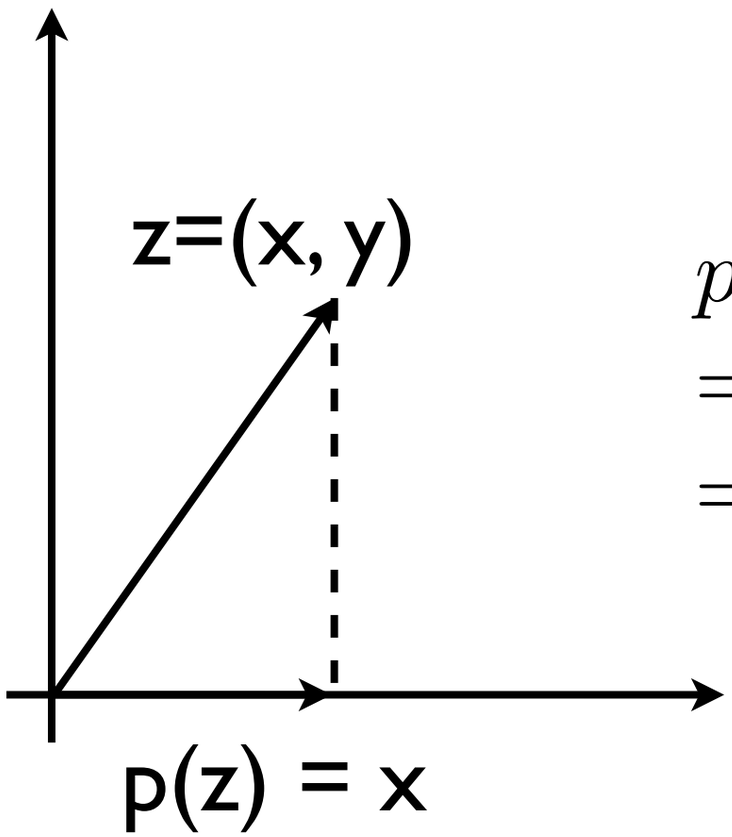
ベクトル空間も群である

- ベクトル空間も群になっている.

  - ２つのベクトルの和はベクトルである.
  - x + (y + z) = (x + y) + z
  - あるベクトルxについてx + 0 = 0 + x = x.　0は零ベクトルとする.
  - あるベクトルxについてx + (-x) = (-x) + x = 0

ベクトルを射影すると準同形

- 2次元のベクトル空間でx軸へ射影してみる



$$p((x,y)) = x$$

$$\begin{aligned} p(z_1 + z_2) &= p((x_1, y_1) + (x_2, y_2)) \\ &= p(x_1 + x_2, y_1 + y_2)) = x_1 + x_2 \\ &= p(z_1) + p(z_2) \end{aligned}$$

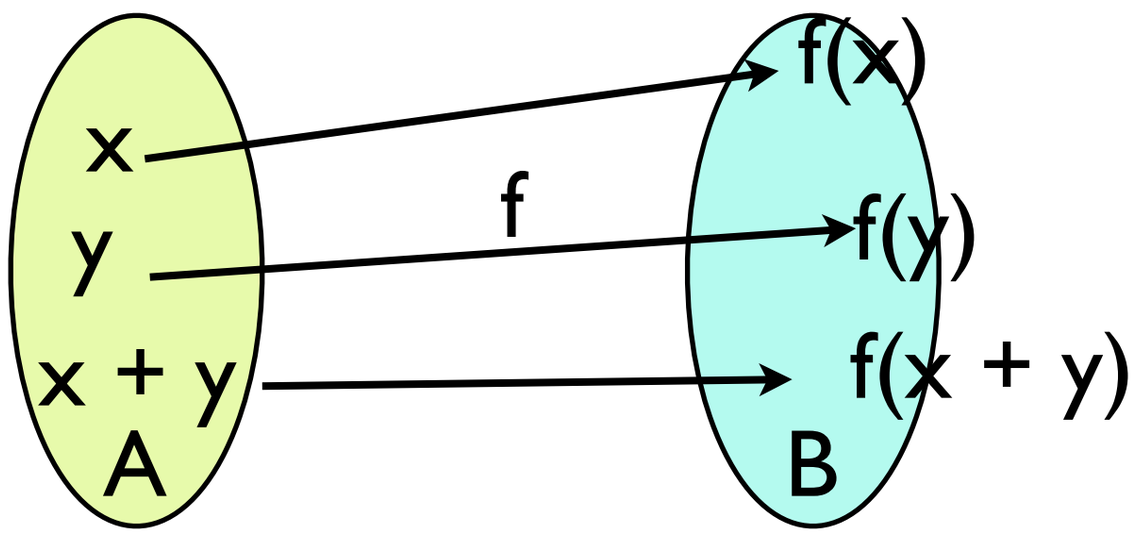
準同形である

準同形 (homomorphism) とは

- 群の準同形とは，２つの群A, Bがあり，AからBへ写像fが定義されているとき，

$$f(x + y) = f(x) + f(y)$$

という構造をもつこと．ただし，左辺の+はAの演算であり，右辺の+はBの演算である．



準同形のカーネルは群をなす(I)

- ２つの群A, Bの間に準同形fが存在すると仮定する.
- このとき，この準同形の核（カーネル）Ker fとは,

$$\mathrm{Ker}\, f = \{x \in A \mid f(x) = 0\}$$

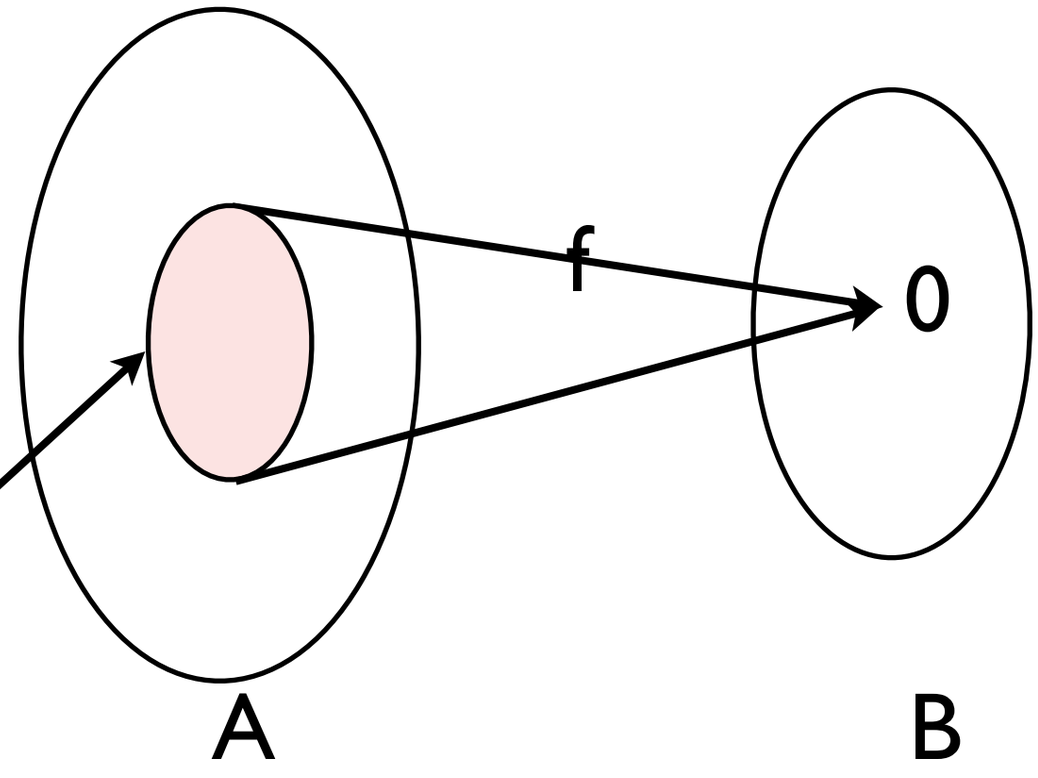
である.

- カーネルは群をなす.

$$f(e) = f(e+e) = f(e) + f(e)$$

カーネルの中に単位元がある

$$f(e) = 0 \longrightarrow e \in \mathrm{Ker}\, f$$



準同形のカーネルは群をなす(2)

- カーネルは演算に関して閉じている

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0$$

$$x, y \in \mathrm{Ker} f \Rightarrow x + y \in \mathrm{Ker} f$$

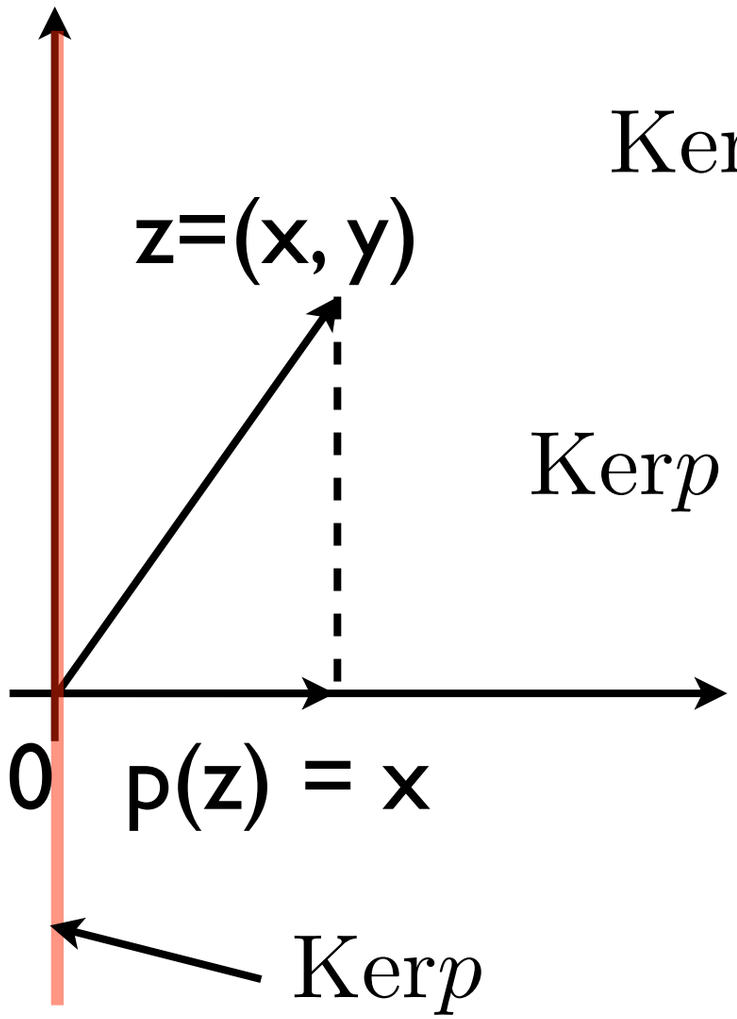
- カーネルは逆元を含む

$$f(x) = 0$$

$$f(x^{-1}) = f(x) + f(x^{-1}) = f(x + x^{-1}) = f(0) = 0$$

カーネルの例 (I)

- 2次元のベクトル空間と射影



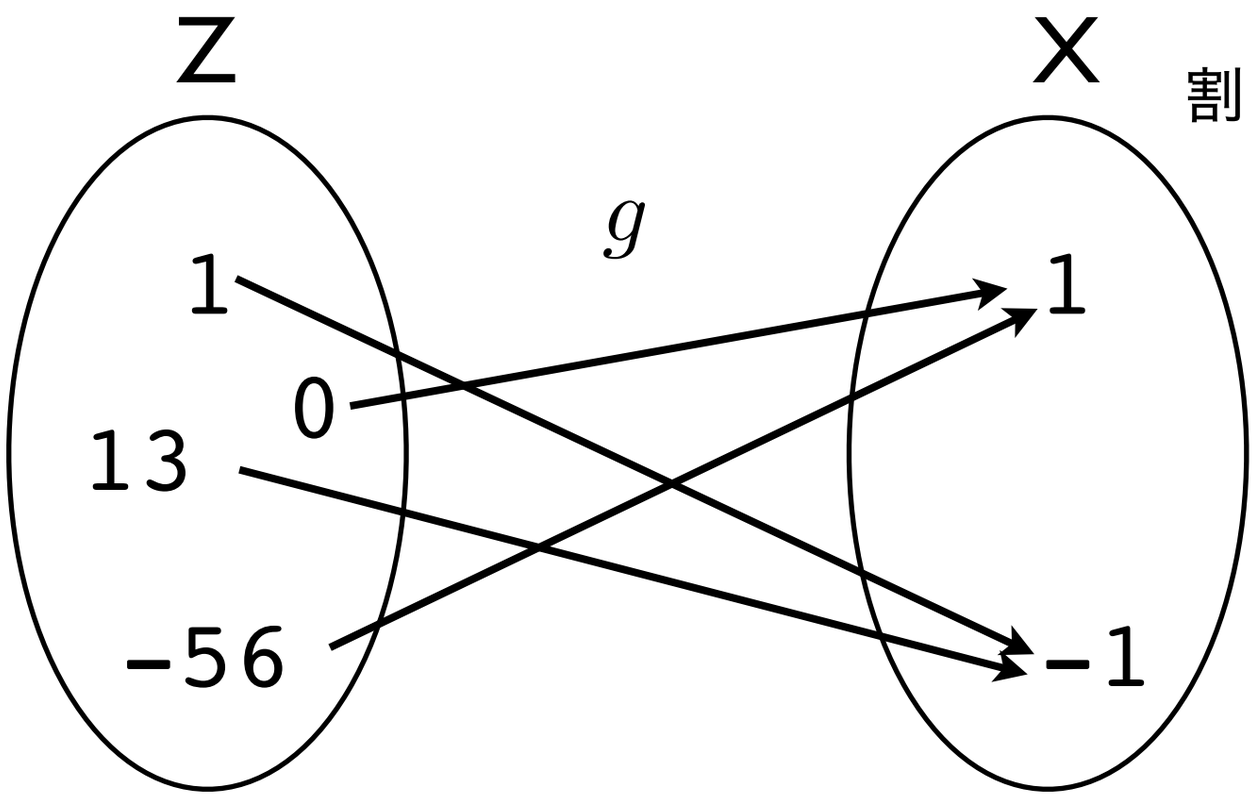
$$\mathrm{Ker}p = \{z = (x, y) \mid \underline{p((x, y))} = 0\}$$

$$= x$$

$$\mathrm{Ker}p = \{(x, y) \mid x = 0\} = \{(0, y) \mid y \in R\}$$

カーネルの例 (2)

- 整数から2で割ったあまりへの準同形



Y = {-1, 1}

$$g(x+y) = g(x)g(y)$$

$g(x) = 1$

↓

カーネルは

偶数の集合

3次の対称群はなぜ群か？(I)

- 以前の考察から3次の対称群は結合則が成り立てば群である：s (t u) = (s t) u
- 実は，この集合の要素は３つの要素の置換であると考えられる

$$
\begin{aligned}
e &= (a \to a, b \to b, c \to c) \\
x &= (a \to b, b \to a, c \to c) \\
y &= (a \to c, b \to b, c \to a) \\
z &= (a \to a, b \to c, c \to b) \\
s &= (a \to b, b \to c, c \to a) \\
t &= (a \to c, b \to a, c \to b)
\end{aligned}
$$

3次の対称群はなぜ群か？(2)

計算方法

$$
\begin{aligned}
xy &= (a \to b, b \to a, c \to c)\,(a \to c, b \to b, c \to a) \\
&= (a \to b, b \to c, c \to a) = s \\
yx &= (a \to c, b \to b, c \to a)\,(a \to b, b \to a, c \to c) \\
&= (a \to c, b \to a, c \to b) = t
\end{aligned}
$$

- 置換は「作用」なので３つの作用を順番にやる場合，どの２つを最初にまとめてみても結果は変わらない．結果が変わらなければ，同じ作用であると考えられる．

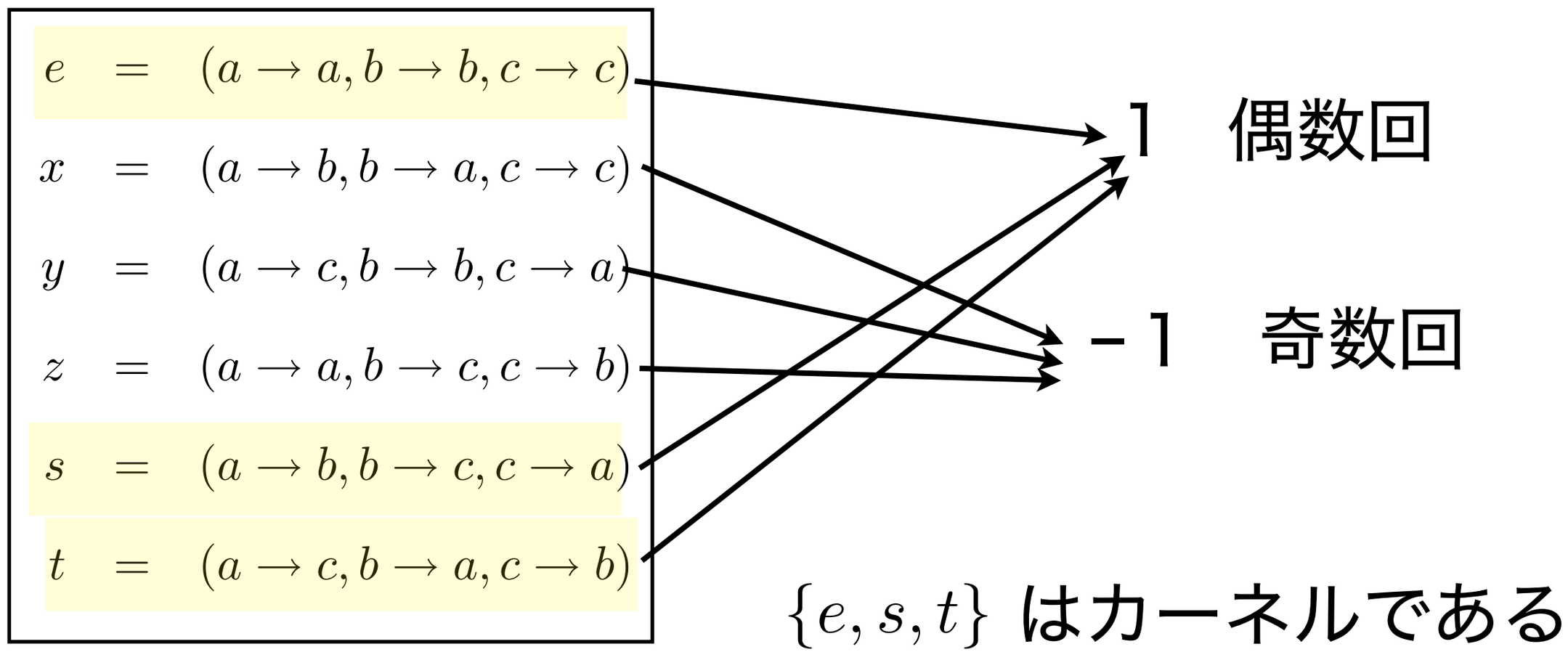
[s (t u)] m = [(s t) u] m

任意のmについて結果が同じならば，同じ作用

3次の対称群から{1，－1}への写像

- 変換が偶数回の互換で表現できるものと奇数回の互換で表現できるものに分かれる

$$
\begin{aligned}
e &= (a \to a, b \to b, c \to c) \\
x &= (a \to b, b \to a, c \to c) \\
y &= (a \to c, b \to b, c \to a) \\
z &= (a \to a, b \to c, c \to b) \\
s &= (a \to b, b \to c, c \to a) \\
t &= (a \to c, b \to a, c \to b)
\end{aligned}
$$



$\{e, s, t\}$ はカーネルである

3次の交代群

よく出ているもう一つの群 -巡回群- (I)

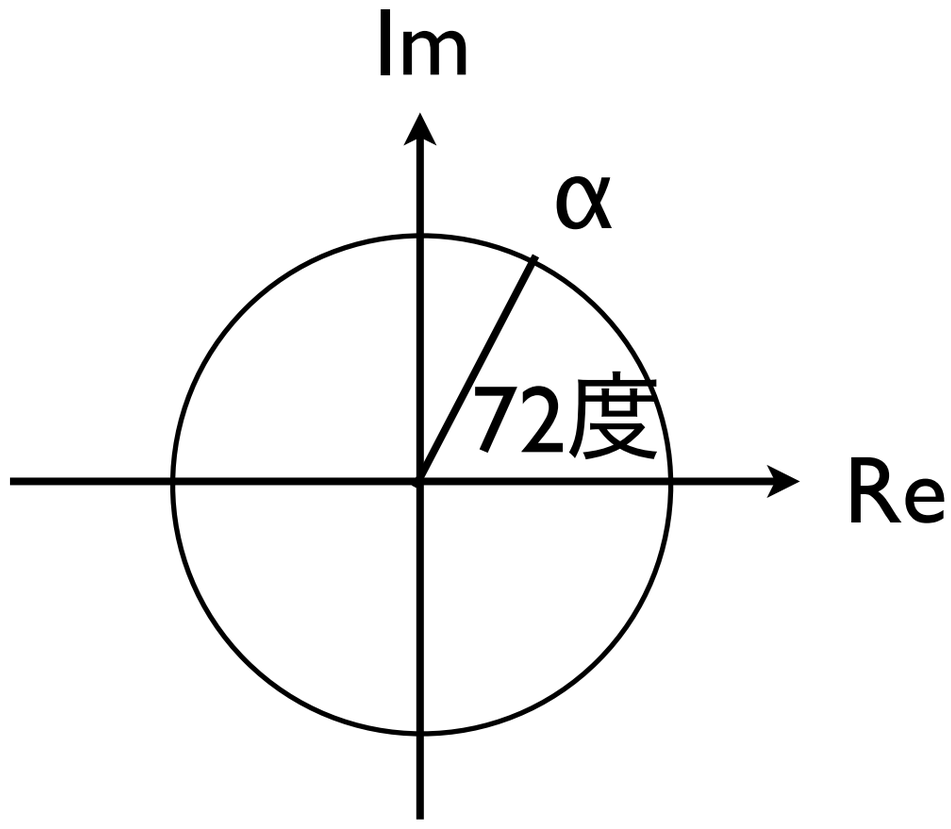
- 巡回群はある程度回ると戻ってくる群

$x^5=x^0 \longrightarrow x^1 \longrightarrow x^2 \longrightarrow x^3 \longrightarrow x^4$

$$\alpha = \sqrt[5]{1}$$

$$G = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$$

$$\alpha = \frac{-1+\sqrt{5}}{4} + \frac{\sqrt{10+2\sqrt{5}}}{4}i$$



よく出てくるもう一つの群 -巡回群- (2)

- もっと単純には虚数単位 i を用いて巡回群を作ることができる.

$$G = \{1, i, i^2 = -1, i^3 = -i\}$$

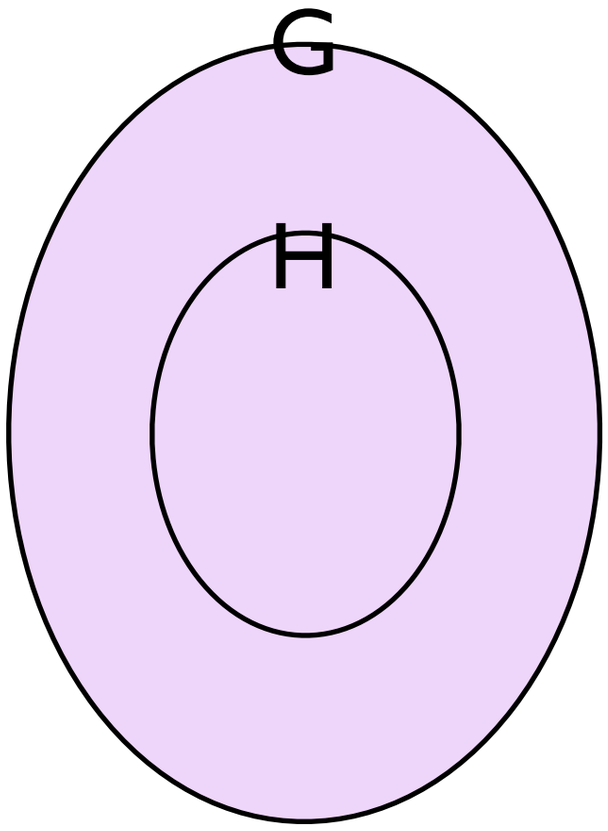
- 一般に $\beta^n = 1$ という性質を仮定して,

$$G = \{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$$

とおけば, これは, 群をなす.

部分群から誘導される同値関係

- ある群に部分群があると，そこから同値関係を定義することができる.



$$x, y \in G$$

$$x \sim y \Leftrightarrow xy^{-1} \in H$$

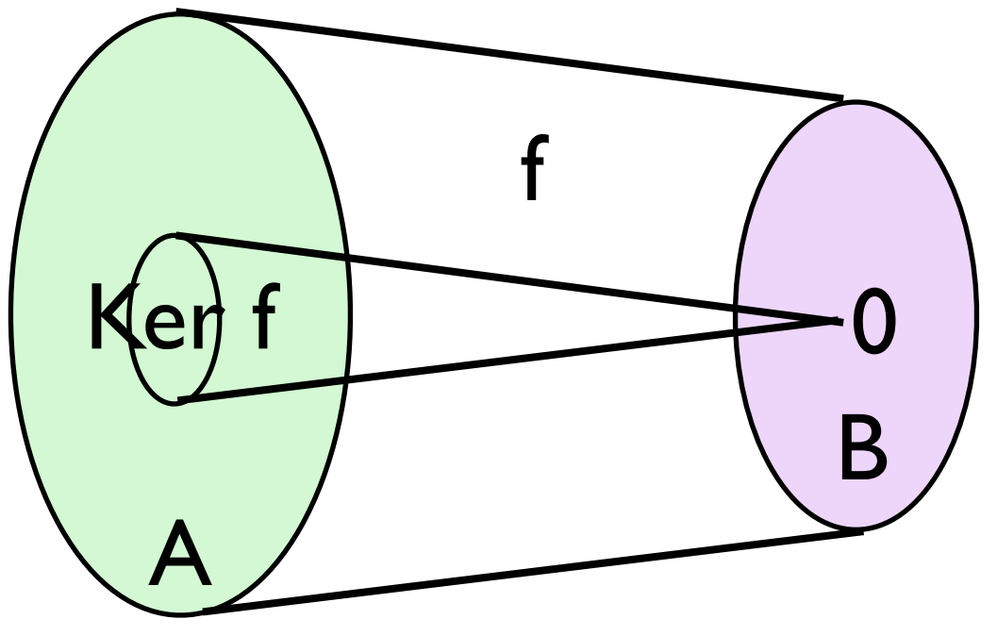
$G/\sim$ のことを G/H と書く

準同形定理

- ２つの群A, Bが存在し，AからBへの準同形fがBへの全射になっているとき,

  A / Ker f ～ B

である．ただし，～は同形であることを表す



準同形定理の例

- A = {0, 1, 2, 3, 4, 5 } として，足して６で割ったあまりを取ると，群になる．この群からB = {0,1}への準同形fを定義する．xが偶数のときf(x) = 0，奇数のときf(x) = 1 とする．Bは2で割ったあまりとする．
- このとき，Ker f = {0, 2, 4}となる．Ker fによって作られる同値関係は a ～ b ⇔ a - b = 0 or 2 or 4. すなわち差が偶数であれば良い．
- これよりAの同値類として{ {0, 2, 4}, {1, 3, 5}} をとることができ，これはBと同形である．

群の表現方法(I)

- 群を表現する一番原始的な方法は要素とその演算表を与えることである.
- もう一つの方法は，要素とその演算規則を与えることである.

ここではこれについて考える

群の表現方法(2)

(生成元)

- 要素とその演算規則をあたえる.

- たとえば,

クラインの4元群であれば,

$$G = \{e, a, b, c\}$$

$$a^2 = e,\ b^2 = e,\ c^2 = e$$

$$ab = bc = c,\ ac = ca = b,\ bc = cb = a$$

$$G = \langle a, b, c \mid a^2, b^2, c^2, abc^{-1}, aba^{-1}b^{-1} \rangle$$

群の表現方法(3)

- 4元群はもっと賢く，つぎのようにも書ける：

$$G = \langle a, b \mid a^2, b^2, aba^{-1}b^{-1} \rangle$$

- 整数の集合は,

$$Z = \langle a \rangle$$

と表現できる.

- 2次元の整数格子は,

$$Z = \langle a, b \mid aba^{-1}b^{-1} \rangle$$

と書ける.

いくつかの特徴的な群

- これから何回か出てくる群を示す

$$\langle a_1, a_2, \cdots, a_n \rangle \quad : \quad \text{自由群} \tag{6.51}$$

$$\langle a_1, a_2, \cdots, a_n \mid a_i a_j a_i^{-1} a_j^{-1} \rangle \quad : \quad \text{自由アーベル群} \tag{6.52}$$

$$\langle a \mid a^n \rangle \quad : \quad \text{巡回群} \tag{6.53}$$

交換しない群は考えづらい

- 交換則の成り立たない群は，全体の構造が見えづらい．特に無限個の要素を持つ群はわかりづらい．実は，交換則が成り立つと，群の構造はかなりすっきりする（アーベルの定理）
- 交換しない群の構造をもう少し単純化することはできないか？

交換子の定義

- 一般に交換しない群の上で，交換子を考える．２つの要素 a, bを指定したとき，その交換子 $[a, b]$ が定義される．

$$[a, b] = a^{-1}b^{-1}ab$$

- もし，もともとa, bの間に交換則が成り立てば，その交換子は単位元になる．

$$a^{-1}b^{-1}ab = a^{-1}ab^{-1}b = ee = e$$

交換子を集めて群をつくる

- 群Gのあらゆる要素によって作られる交換子をあつめた集合をX(G)とおく.

$$[a,b] = a^{-1}b^{-1}ab$$

$$X(G) = \{[a,b] \mid a,b \in G\}$$

- X(G)が群になるとは限らないが, この集合の要素から群を生成することができる. これをD(G)と書き, Gの**交換子群 (comutator group)** と呼ぶ.

- D(G)は明らかにGの部分群である.

交換子群の成り立ち

- X(G)は群になるとは限らないが，単位元を含む．なぜならば，[a, a] = e であるからである．
- X(G)の元 [s, t] の逆元は [t, s]であるので，この逆元も含む．
- X(G)の要素から演算によって生成される要素をすべて含めれば D(G) が得られる．

交換子群の性質 (I)

- 群Gの任意の要素 t について $t^{-1}D(G)t = D(G)$ である.

$$\boxed{\phi(x) = t^{-1}xt}$$

$$t^{-1}[a,b]t = t^{-1}a^{-1}b^{-1}abt = t^{-1}a^{-1}tt^{-1}b^{-1}tt^{-1}att^{-1}bt$$
$$= [t^{-1}at, t^{-1}bt] \in D(G)$$

φは単射

φはD(G)の内部に写像する

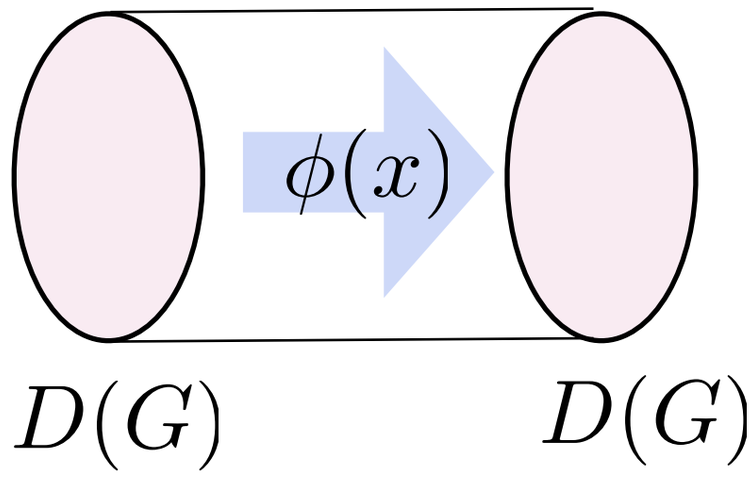
はみ出ない

$$\phi(x) = \phi(y) \Leftrightarrow t^{-1}xt = t^{-1}yt \Rightarrow x = y$$

φは全射

$$\phi(x) = y \Rightarrow x = tyt^{-1} \in D(G)$$

φは全単射（１対１の対応）



交換子群の性質 (2)

- tをGから選び，aをG(D)から選ぶとき,

$$ta = bt$$

となるbをG(D)から選択することができる．なぜならば,

$$tat^{-1} = b$$

と書けるからである.

交換子群を用いた同値関係

- a ～ b を以下のように定義すると，～は同値関係になる.

$a, b \in G$

$$\boxed{a \sim b \Leftrightarrow ab^{-1} \in D(G)}$$

$a \sim a$ $aa^{-1} = e \in D(G)$

$a \sim b \Rightarrow b \sim a$ $ab^{-1} \in D(G) \Rightarrow ba^{-1} = (ab^{-1})^{-1} \in D(G)$

$a \sim b, b \sim c \Rightarrow a \sim c$ $(ab^{-1})(bc^{-1}) = ac^{-1} \in D(G)$

交換子群による同値関係の同値類

- ～は同値関係なので，　～を用いてGを分類することができる.

- 同値な要素どうしでグループを作る

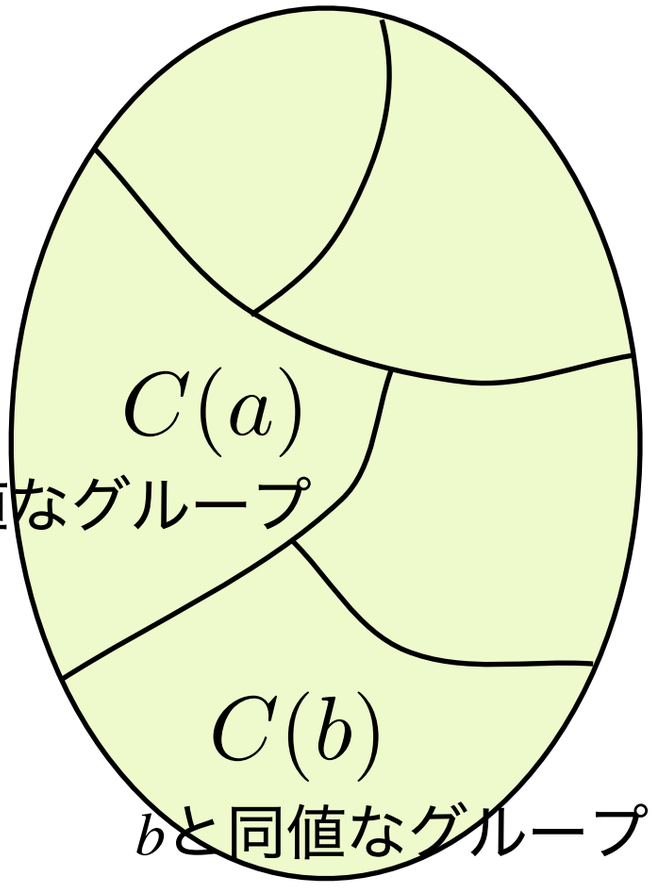
$$b = nb_1 \qquad b \sim b_1$$
$$a = ma_1 \qquad a \sim a_1$$
$$n, m \in D(G)$$

$$ab = ma_1nb_1 = mn'a_1b_1$$

$$ab \sim a_1b_1$$

適当なD(G)の要素

グループどうしの演算が定義できる



１つのグループを１つの要素にした群（商群）

- グループどうしの演算が定義できるので，その演算に関するグループの演算によって群が作れる.

$$nema = nma \sim a$$

$$(na)^{-1} = a^{-1}n^{-1} = n'a^{-1} \sim a^{-1}$$

- この群のことをG/D(G)と書く.

G/D(G)は可換群である

- 実は，G/D(G)は可換群になる．これはabとbaが同じグループに入ることから得られる.

$$ab = ba(a^{-1}b^{-1}ab) = ba[a, b]$$

$$ab \sim ba$$

- この群のことをGの**可換化 (Abelianization)**と呼ぶ
- もとの群からの作り方は唯一なので，同じ群ならば可換化したものも同じはずである．結果が可換群なので扱いやすい.