群・環・体 速習講座

@yfbk271_chigu

概要

速習と書いておきながら，長々と書いてしまった．ある程度まで，書いたので群のみ公開する．
いずれ，環，体，そして Galois の基本定理まで扱おうと思っている．何ヶ月掛かるかわからないのが現状である．が，気長に待ってくれるとありがたい．必ず完成させよう．

目次

1　群

1.1　群の定義

最小限の知識のみ記しておく．

Definition 1.1.1.

G を空集合でない集合とする．G 上の演算が定義されていて次の性質を満たす時，G を群という．

(1) 単位元と呼ばれる元 $e \in G$ が存在し，すべての $a \in G$ に対し $ae = ea = a$ となる．
(2) すべての $a \in G$ に対し $b \in G$ が存在し，$ab = ba = e$ となる．この元 b は a の逆元とよばれ，a^{-1} と表す．
(3) すべての $a, b, c \in G$ に対し，$(ab)c = a(bc)$ が成り立つ．

これらの演算は所謂，掛け算とは異なった概念であることを認識しておいてほしい．

交換法則も成り立つとき，G は可換であるといい，可換群，アーベル群，加群という．ただし，後に，A–加群と呼ばれる概念が登場するため，加群という言葉は以下において使わないことにする．
G が群であるとき，その元の個数を $|G|$ とかき，これを G の位数とよぶ．

単位元の一意性，簡約法則についてはここでは省く．

1.2　置換群

X を集合とするとき，X から X への全単射写像 $\sigma : X \to X$ のことを X の置換という．σ, τ を X の 置換とするとき，その積，$\sigma\tau$ を写像としての合成 $\sigma \circ \tau$ と定義する．これは演算をするとき，$\sigma(\tau)$ のように考えるとわかりやすい．

Definition 1.2.1.

X の置換全体からなる群のことを X の置換群という．$X_n = \{1, 2, \cdots, n\}$ とするとき，X_n の置換のことを n 次の置換という．n 次の置換全体よりなる群のことを $\mathfrak{S}_n$ であらわし，$\mathfrak{S}_n$ を n 次対称群という．これは位数 $n!$ の有限群である．

Example 1.2.2.

$G = \mathfrak{S}_n$ とおく，このとき，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \in G$$

は $1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 4,\ 4 \mapsto 2$ となる元である．

$1 \leq i_1, i_2, \cdots, i_m \leq n$ を全て異なる整数とするとき，

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_m \mapsto i_1$$

と写し，他の $1 \leq j \leq n$ は変えない置換を $(i_1 \cdots i_m)$ と表し，長さ m の巡回置換という．例 1 の置換を巡回置

換を用いて表すと，(1342) である．$1 \leq i < j \leq n$ のとき，$l \neq i, j$ なら $\sigma(l) = l$ で $\sigma(i) = j, \sigma(j) = i$ であるとき，σ は置換である．このような置換を i, j の互換といい (ij) で表す．
例 1.2.2 の置換を互換を用いて表すと，(12)(14)(13) である．このことから想像できるように，一般に巡回置換は互換の積で表せる．
この置換群という概念は，Galois 群 において非常に有用である．是非覚えておいてほしい．

1.3 元の位数

Definition 1.3.1.

G を群，$g \in G$ とする．
(1) $g^n = 1$ となる $n > 0$ があれば，そのような n の最小値を g の位数という．
(2) $g^n = 1$ となる $n > 0$ がなければ，g の位数は ∞ という．

Proposition 1.3.2.

G を群，$g \in G$ を位数が有限である元とする．このとき，$m \in \mathbb{Z}$ に対して以下の二つは同値．
(1) $g^m = 1$.
(2) m は n の倍数.

Proof. $k \in \mathbb{Z}$, $m = kn$ なら，$g^m = (g^n)^m = 1$ である．
逆に $g^m = 1$ とする．m が n の倍数でないと仮定し，$m = qn + r$ と割り算すると，$0 < r < n$ である．$1 = g^m = (g^n)^q g^r$ となるんので，n が g の位数であることに反する．よって m は n の倍数. □

1.4 部分群

Definition 1.4.1.

G を群とする．G の空でない部分集合 H が G の演算で群になる時，H を G の部分群という．

Proposition 1.4.2.

群 G の部分集合 H が G の部分群になるための必要十分条件は，任意の $x, y \in H$ に対して，$xy^{-1} \in H$ が成り立つことである．

Proof. H が G の部分群のとき，$y \in H$ の逆元 $y^{-1} \in H$ が存在し，H の演算は閉じているので $xy^{-1} \in H$ である．逆に，$x, y \in H$ に対して，$xy^{-1} \in H$ が成り立つとき，$x = y$ であれば $xy^{-1} = e$ で単位元が存在し，$x = e$ であれば，$y^{-1} \in H$ であるから逆元も存在する．最後に，G で結合法則が成り立つので H でも結合法則が成り立つことは自然なことである．よって H は G の部分群である. □

Definition 1.4.3.

部分集合 $S \subset G$ に対し，S の元，あるいはその元の逆元の有限個の積により，なる G の部分集合を $\langle S \rangle$ とする．つまり，$\langle S \rangle$ は $x_1, \cdots x_t \in S$ により $x_1^{\pm 1} \cdots x_t^{\pm 1}$ という形をした元全体の集合である．

Proposition 1.4.4.

$\langle S \rangle$ は G の部分群である．

Proof. $1 \in \langle S \rangle$ $x_1, \cdots x_n, y_1, \cdots y_n \in S$ なら，

$$\left(x_1^{\pm 1} \cdots x_n^{\pm 1}\right)\left(y_1^{\pm 1} \cdots y_n^{\pm 1}\right) = x_1^{\pm 1} \cdots x_n^{\pm 1} y_1^{\pm 1} \cdots y_n^{\pm 1} \in \langle S \rangle$$

$x_1^{\pm 1} \cdots x_n^{\pm 1}$の逆元 $x_1^{\mp 1} \cdots x_n^{\mp 1} \in \langle S \rangle$ である．したがって，題意は示された． □

$\langle S \rangle$ を S で生成された部分群といい，S を $\langle S \rangle$ の生成系，S の元を生成元という．G が一つの元で生成される時，G を巡回群という．群の部分群で巡回群であるものは巡回部分群という．

Example 1.4.5.

$\mathbb{Z}$ は $\langle 1 \rangle$ で生成される位数 ∞ の巡回無限群である．また，$n\mathbb{Z}$ は n を生成元とする $\mathbb{Z}$ の位数 ∞ の巡回無限部分群である．

Proposition 1.4.6.

g が群 G の位数を $n > 0$ とする元であるとき，$\langle g \rangle$ の位数は n である．

Proof. 自明. □

1.5 準同型

Definition 1.5.1: 準同型・同型

G_1, G_2 を群，$\phi : G_1 \to G_2$ を写像とする．
(1) $\phi(xy) = \phi(x)\phi(y)$ が $\forall x, y \in G_1$ に対して成り立つ時，ϕ を準同型という．
(2) ϕ が準同型で逆写像を持ち，逆写像も準同型であるとき，ϕ を同型といい $G_1 \cong G_2$ と表す．
(3) ϕ が準同型の時，$\mathrm{Ker}(\phi) = \{x \in G_1 \mid \phi(x) = 1_{G_2}\}$ を ϕ の核という．
(4) ϕ が準同型の時，$\mathrm{Im}(\phi) = \{\phi(x) \mid x \in G_1\}$ を ϕ の像という．

Proposition 1.5.2.

全単写写像 $\phi : G_1 \to G_2$ が群の準同型なら，同型である．

Proof. ϕ の逆写像を ψ とおく．$x, y \in G_2$ とすると ϕ は準同型なので，

$$\phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\phi(y)) = xy = \phi(\psi(xy))$$

となり，ϕ は単射なので，ψ は準同型である． □

Proposition 1.5.3.

$\phi : G_1 \to G_2$ を群の準同型とする時，次が成り立つ．
(1) $\phi(1_{G_1}) = 1_{G_1}$
(2) $\forall x \in G_1, \phi(x^{-1}) = \phi(x)^{-1}$
(3) $\mathrm{Ker}(\phi), \mathrm{Im}(\phi)$ はそれぞれ G_1, G_2 の部分群．

Proof.
(1) $\phi(1_{G_1}) = \phi(1_{G_1} \cdot 1_{G_1}) = \phi(1_{G_1})\phi(1_{G_1})$ より，$\phi(1_{G_1})$ がわかる．
(2) $\phi(1_{G_1}) = \phi(x \cdot x^{-1}) = \phi(x)\phi(x^{-1})$ より，$\phi(1_{G_1}) = \phi(x)\phi(x^{-1})$ の両辺に $\phi(x)^{-1}$ を右側から作用させることで $\phi(x^{-1}) = \phi(x)^{-1}$ がわかる．
(3) $x, y \in \mathrm{Ker}(\phi)$ とすると，$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = 1_{G_2} \cdot 1_{G_2} = 1_{G_2}$ である．よって，1.4.2 から，G_1 の部分群である．
また，$1_{G_2} = \phi(1_{G_1}) \in \mathrm{Im}(\phi), \forall x, y \in G_1$ に対し，$\phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} \in \mathrm{Im}(\phi)$ である．よって，ϕ は G_2 の部分群である． □

Example 1.5.4.

群 $G \ni x, \mathbb{Z} \to G, \phi(x) := n^x$ とすると，ϕは準同型．また，d を x の有限位数とすると，$\mathrm{Im}(\phi) = \langle x \rangle$

Proposition 1.5.5.

(1) 群の準同型写像の合成は準同型写像．
(2) 群の同型写像の合成は同型写像であり，同型写像の逆写像も同型写像．

Proposition 1.5.6.

$\phi : G_1 \to G_2$が準同型である時，次の二つは同値．
(1) ϕは単射．
(2) $\mathrm{Ker}(\phi) = \{1_{G_1}\}$

Proof. (1) → (2) : ϕが単射であるとすると，$1_{G_1} \in \mathrm{Ker}$ は明らか．$\mathrm{Ker}(\phi)$ なら$\phi(g) = 1_{G_2} = \phi(1_{G_1})$ であるがϕは単射なので，$g = 1_{G_1}$.よって (2) は成り立つ．
(2) → (1) : $\mathrm{Ker}(\phi) = \{1_{G_1}\}$ とする．$g, h \in G_1, \phi(g) = \phi(h)$ なら，$\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = 1_{G_2}$.よって，$gh^{-1} \in \mathrm{Ker}(\phi) = \{1_{G_1}\}$ であり，$g = h$ なので，ϕは単射． □

1.6 同値と剰余

Definition 1.6.1.

集合 S 上の関係 $\sim$ が $\forall a, b, c \in S$ に対して次の条件を満たす時，同値関係という．

(1) $a \sim a$

(2) $a \sim b$ なら $b \sim a$

(3) $a \sim b, b \sim c$ なら $a \sim c$

Example 1.6.2.

$\exists n \in \mathbb{Z}_{>}, x, y \in \mathbb{Z}, n \mid x - y$ のとき，$x \equiv y \bmod n$ と定義すると，このとき同値関係が成り立つことは容易にわかる．

ちなみに，$\exists n \in \mathbb{Z}_{>}, x \in n\mathbb{Z}$ と定義した時，$x^{-1} \notin \mathbb{Z}$ と考えてしまう人がいるが，このとき x^{-1}は $-x$ と同値であり，逆元は存在する．これは $n\mathbb{Z}$ が加法に関して群をなしているからである．

Definition 1.6.3.

$\sim$ を集合 S 上の同値関係とする．$x \in S$ に対し，

$$C(x) = \{y \in S \mid y \sim x\}$$

を x の同値関係という．

Proposition 1.6.4.

$\sim$ を集合 S 上の同値関係，$C(x)$ を $x \in S$ の同値類とする．

(1) $\forall y, z \in C(x)$ に対し，$y \sim z$ である．

(2) $y \in C(x)$ なら $C(x) = C(y)$

(3) $x, y \in S, C(x) \cap C(y) \neq \varnothing$ なら $C(x) = C(y)$

Proof. (1) 自明．

(2) $y \in C(x)$ とする．$x \in C(x)$ なら，$x \sim y$ より，$C(x) \subset C(y)$．$x \in C(y)$ なので同様に，$C(y) \subset C(x)$．よって，$C(x) = C(y)$．

(3) $x, y \in S, x \in C(x) \cap C(y)$ なら (2) より，$C(x) = C(z), C(y) = C(z)$ であるから，$C(x) = C(y)$． □

これらのことから，$S = \coprod_{x \in S} C(x)$ も直ちにわかる．

Definition 1.6.5.

H を群 G の部分群，$x \in G$ とする．

H の左剰余類を G の部分集合である，

$$xH = \{xh \mid h \in H\}$$

と定義する．同様にして右剰余類は $Hx = \{hx \mid h \in H\}$ と定義される．このとき，x は代表元と言われる．

Example 1.6.6.

$G = \mathfrak{S}_3, H = \langle (1\ 2) \rangle$ とすると，H の右剰余類は

$$H = \{1, (1\ 2)\}, H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}, H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}$$

左剰余類は

$$H = \{1, (1\ 2)\}, (1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}, (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}$$

例からわかるように，H の右剰余類と左剰余類は一致しない場合がある．
群 $G \ni x$,G の部分群 H の右剰余類 Hx の集合を $H\backslash G$，同様に xH の集合を G/H と表す．

1.7 ラグランジュの定理

Definition 1.7.1.

~ を集合 S 上の同値関係とする．
(1) S の部分集合で $C(x)(x \in S)$ と表せるもの全体の集合を $S/\sim$ と表す．
(2) S の部分集合 R が $S/\sim$ の同値類の代表元を一つずつのみ含むとき，R を ~ の完全代表系という．

Example 1.7.2.

$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$ である．このとき，完全代表系の一つは $\{0, 1, 2, 3, 4, \}$ である．また，$\{10, 11, 12, 13, 14\}$ も完全代表系の一つである．

Proposition 1.7.3.

H が群 G の部分群であるとすると，次の二つが成り立つ．
(1) $|G/H| = |H\backslash G|$
(2) $\forall g \in G, |gH| = |Hg| = |H|$

例 1.6.6 を見ると明らかだろう．

Definition 1.7.4.

$G/H, H\backslash G$ の元の個数を $(G : H)$ と表し，これを H の G における指数という．

Theorem 1.7.5: ラグランジュの定理

$|G| = (G : H)|H|$ が成り立つ．

Proof. G/H の完全代表系 $\{\varepsilon_i\}$ をとると，$G = \coprod_i \varepsilon_i H$ が成り立つ．$\forall i$ に対し $|\varepsilon H| = |H|$ より，定理が従う． □

Corollary 1.7.6.

G を有限群とするとき，次の (1), (2) が成り立つ．
(1) H が G の部分群なら，$|H|$ は $|G|$ の約数．
(2) $g \in G$ の位数は $|G|$ の約数．

Probrem 1.7.7: Fermat の小定理

$p \in \mathbb{F}, p \nmid x \in \mathbb{Z}$ なら $x^{p-1} \equiv 1 \bmod p$ であることを示せ．

1.8 正規部分群

Definition 1.8.1.

H を群 G の部分群とする．$\forall g \in G, h \in H$ に対し $ghg^{-1} \in H$ となる時，H を G の正規部分群といい，$H \triangleleft G$ とあらわす．

Example 1.8.2.

G が可換群で H が任意の部分群の時 $gh^{-1} = h \in H$ なので，H は正規部分群である．$2\mathbb{Z}.3\mathbb{Z} \subset \mathbb{Z}$ などは正規部分群．

Proposition 1.8.3.

G_1, G_2が群で$\phi : G_1 \to G_2$が準同型なら $\mathrm{Ker}(\phi)$ は G_1の正規部分群である．

Proof. $g \in G_1, h \in \mathrm{Ker}(\phi)$ とすると，

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1_{G_2}$$

であり，$ghg^{-1} \in \mathrm{Ker}(\phi)$ のため，$\mathrm{Ker}(\phi) \triangleleft G_1$である． □

Lemma 1.8.4.

H が G の部分群なら，次の二つの主張は同値である．
(1) H は G の正規部分群である．
(2) $\forall g \in G$ に対し，$gH = Hg$ である．

Proof. (1) $\Rightarrow$ (2) $h \in H$ なら，$h' = ghg^{-1} \in H$ である．よって，$gh = h'g \in Hg$ である．これは，$\forall h$ に対して成り立つため，$gH \subset Hg$ である．同様に，$Hg \subset gH$ であるため，$gH = Hg$ が成り立つ．
(2) $\Rightarrow$ (1) $g \in G, h \in H$ なら，$gn \in gH = Hg$ より，$\exists h' \in H, gh = h'g$ が成り立つ．よって，$ghg^{-1} = h' \in H$ であるため，H は正規部分群である． □

この補題から正規部分群とは左剰余群と右剰余群が一致するということを示している.

Proposition 1.8.5.

H を群 G の正規部分群, x, y を G の代表元とすると,

$$(xH)(yH) = xyH$$

が成り立つ.

Proof. $h, h' \in H$ とすると, $xhyh' \in (xH)(yH)$ である. $xhyh' = xy(y^{-1}hy)h$ より, $\exists h'' \in H$ に対して $y^{-1}hy = h''$が成り立つ. よって, $xhyh' = xyh''h \in xyH$ である. □

Proposition 1.8.6.

N を G の正規部分群とした時, G/N は命題 1.8.5 の演算により群をなす.

Proof. N が単位元となるのは明らか. 先の命題より結合法則が成り立つのは明らか. 逆元の存在は明らか. □

Proposition 1.8.7.

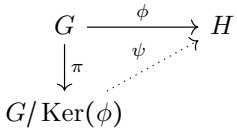
H を群 G の正規部分群とすると, $\phi : G \to G/H$ は群の全写準同型であり, $\mathrm{Ker}(\phi) = H$ である.

Proof. $x, y \in G, \phi(x) \coloneqq xH$ とすると, $\phi(xy) = \phi(x)\phi(y) = xHyH = xyH$ であり, この写像は全写である. また, G/H の単位元は H であるから, $g \in \mathrm{Ker}(\phi), \phi(g) = gN = N$ より, $\mathrm{Ker}(\phi) = N$ であることは明らか. □

1.9 準同型定理

Theorem 1.9.1: 準同型定理 (第一同型定理)

$\phi : G \to H$ を群の準同型とする. $\pi : G \to G/\mathrm{Ker}(\phi)$ を準同型とするとき, 下図が可換図式[a]となるような準同型 $\psi : G/\mathrm{Ker}(\phi) \to H$ がただ一つ存在し, ψ は $G/\mathrm{Ker}(\phi)$ から $\mathrm{Im}(\phi)$ への同型となる.



[a] 等しい集合間の異なる経路の写像の合成が等しくなる時, 図は可換図式であるという.

Proof. $x, y \in G, \mathrm{Ker}(\phi) = K$ とする. 命題 1.8.3 より, $\mathrm{Ker}(\phi)$ は G の正規部分群である. ψ が準同型であることを示す.

Lemma 1.9.2.

$xK = yK \Leftrightarrow y^{-1}x \in K$ である．

Proof. $(\Rightarrow)$ $xK = yK \Leftrightarrow K = y^{-1}xK$．$K$ は群であるから，$h \in K$ に対して ,$\exists h' \in K$ であり，$h = y^{-1}xh'$ が成り立つ．
$(\Leftarrow)$ $\phi(y^{-1}x) = \phi(y^{-1})\phi(x) = \phi(y)^{-1}\phi(x) = 1_H$．よって，$\phi(y)^{-1}\phi(x) = 1_H \Leftrightarrow \phi(x) = \phi(y)$. □

補題より，$\psi(xK) = \phi(x)$ という写像を考える．これは，$\psi : G/K \to H$ の対応が定まり，ψ は単写であることがわかる．また，K は正規部分群であるから，

$$\psi(xKyK) = \psi(xyK) = \phi(xy) = \phi(x)\phi(y) = \psi(xK)\psi(yK)$$

よって，ψ は準同型である．写像 π は命題 1.8.7 から明らか．$\psi(xK) = \phi(x)$ が全写であることは明らか．よって全単写であり，$G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$ である． □

Example 1.9.3.

$G := \langle x \rangle, |G| = n$．$\phi : \mathbb{Z} \ni m \mapsto x^m \in G$ とする．これが準同型なのは明らか．x は生成元なので全写であることは明らか．$\mathrm{Ker}(\phi) = n\mathbb{Z}$ なので第一同型定理より，$\mathbb{Z}/n\mathbb{Z} \cong G$ である．

Theorem 1.9.4: 第二同型定理

H, N を群 G の部分群，$N \triangleleft G$ と定める．この時，次の $(1), (2)$ が成り立つ．
(1) HN は G の部分群であり，$HN = NH$ である．
(2) $H \cap N \triangleleft H, HN/N \cong H/H \cap N$.

Proof. (1) $h, h' \in H, n, n' \in N$ とする．$(hn)(h'n')^{-1} \in hNh'^{-1}N = hh'^{-1}NN \subset HN$．また，補題 1.9.2 より，$HN = NH$ は明らか．
(2) $x \in H$ とする．$H \to HN/N$ となる写像 $\phi(x) = xN$ は全写準同型である．$\mathrm{Ker}(\phi) = H \cap N$ なので同様に，$H \cap N \triangleleft H$ であり，第一同型定理より，$HN/N \cong H/H \cap N$ である． □

Theorem 1.9.5: 第三同型定理

G を群，$G \triangleright N \subset N'$ とするとき，次の $(1), (2)$ が成り立つ．
(1) 準同型写像 $\phi : G/N \to G/N'$ で $\phi(xN) = xN'$ となるものが存在する．
(2) $(G/N)(N'/N) \cong G/N'$

Proof. 第一同型定理より自明． □

参考文献

[1] 雪江明彦,『群論入門』(代数学 1),日本評論社,2010.

[2] 雪江明彦,『環と体のガロア理論』(代数学 2),日本評論社,2010.

[3] M. F. Atiyah, L. G.MacDonald (著),新妻弘 (訳),『Atiyah-MacDonald 可換代数入門』,共立出版,2006.

[4] J. Rotman (著),関口次郎 (訳),『改訂新版 ガロア理論』,丸善出版,2012.

[5] 齋藤正彦,『線形代数入門』,東京大学出版,1966.