代数学Ｉ・代数学演習Ｉ

明治大学理工学部数学教室

２００１年度版

目　次

はじめに.

群の理論である「群論」はそれ自体で完結した体系であるのみでなく, 代数系構築の基本パターンであり, しかも数学の基本構造の一つでもある. その上数学の様々な場面で色々な役割を担って群が登場し, その分野の要となることも多い. 例えば 5 次以上の代数方程式には根の公式が存在しないという, Abel の定理は方程式の分解体の自己同型群の構造を解析することによって証明される. 群とその理論が数学という学問において果たす役割は多面的であるため, 群の定義そのものは至って単純であるにも拘わらず, 数学の学習が進むに連れて次々と展開されてゆく群論を立体的に俯瞰することは必ずしも容易ではない. この意味では美と同様に真理 (学問) も瞰る者の眼の中にしか存在しないのである. 群論を学ぶ者は, この体系が多方面の数学で様々な役割を果たしていることを念頭におきつつ, 公理から出発して少しずつ理論を構築しながら, 一日も早くひとまずは完結した体系となるよう努力することが肝要である.

問題を解く上での注意

同じタイプの問題 (問題番号の右上に同じアルファベットの付いている問題) を一人で二問以上解いてはならない. 一つの問が 1), 2), 3) のように幾つかに別れている場合は一人で全部解くこと.

§1 同値関係 (equivalence relation)

ものの集まりを全体として一つの対象と見做すときこれを**集合** (a set) と呼ぶ. 集合を表すには大文字の A, B, C, $\cdots$, X, Y, Z を使うことが多い. これに対して集合の元の方は小文字 a, b, c, $\cdots$, x, y, z を用いて表すことが普通である. 例えば 4 つの数 1, 2, 3, 4 からなる集合を A とすれば, $A = \{1, 2, 3, 4\}$ であって, 1, 2, 3, 4 はそれぞれ集合 A の**元** (an element) である. 即ち 1, 2, 3, $4 \in A$. 実数全体を一つの対象と考えこれを一つの集合と見做すときには通常は記号 $\boldsymbol{R}$ を用いる. $\boldsymbol{R}^3 = \{(a, b, c) \mid a, b, c \in \boldsymbol{R}\}$ とおき, $\boldsymbol{R}^3$ の元を直交座標系の入った空間の点と同一視すれば, 集合 $\boldsymbol{R}^3$ は極めて多様な構造を持った数学的対象となる. あるものの集まり全体を一つの対象と捉えて集合と見做すときは, その集合にいかなる数学的構造を入れて考えようとしているかが大切である.

二つの集合 A, B は要素を完全に共有するとき同じものであると考える. 即ち A は B の**部分集合** (a subset) であって, かつ B も A の部分集合であるとき $A = B$ であると定める. 集合 A, B に対して $A \times B = \{(a, b) \mid a \in A, b \in B\}$ と置き A と B の**直積集合** (the direct product of A and B) と呼ぶ. さて A は空でない集合としよう. 直積集合 $A \times A$ の部分集合のことを集合 A の上の**関係** (a relation on A) と呼ぶ. R が集合 A の上の一つの関係であれば, A の二つの元 a, b については, 組 (a, b) が R の元であるかあるいは R の元でないかは, 考えている関係 R の定義によって明確に定まっている. いま組 (a, b) が R の元であることを簡単のため $a\mathrm{R}b$[1] と書き a アール b と読むことにする. 例えば $\boldsymbol{Z}$ を整数全体のなす集合とし,

$$\mathrm{R} = \{(a, b) \mid a, b \in \boldsymbol{Z} \text{ であって } a - b \text{ は } 7 \text{ の倍数である } \}$$

と置けば R は直積 $\boldsymbol{Z} \times \boldsymbol{Z}$ の部分集合であって, 集合 $\boldsymbol{Z}$ の上の一つの関係となる. $(4, 11)$ は R の元であるから 4R11 である. 同様に 1R(-6) である.

定義 1.1. A は空でない集合とし R を A 上の関係とする. 次の 3 条件が満たされるとき, R は A 上の**同値関係** (an equivalence relation on A) であるという.

1) (反射律) A の全ての元 a について $a\mathrm{R}a$ である.
2) (対称律) $a, b \in A$ とするとき, $a\mathrm{R}b$ であれば $b\mathrm{R}a$ でもある.
3) (推移律) $a, b, c \in A$ とするとき, $a\mathrm{R}b$ であってかつ $b\mathrm{R}c$ であれば $a\mathrm{R}c$ である.

例えば上の関係 $\mathrm{R} = \{(a, b) \mid a, b \in \boldsymbol{Z} \text{ であって } a - b \text{ は } 7 \text{ の倍数である } \}$ は $\boldsymbol{Z}$ 上の同値関係である. さて空でない集合 A の上に同値関係 R が一つ与えられているものと仮定する. A の元 a に対して

$$\mathrm{C}(a) = \{x \mid x \in A \text{ であって } x\mathrm{R}a \text{ である } \}$$

と置き, この集合 $\mathrm{C}(a)$ を a を含む**同値類** (the equivalence class of a) という. 集合 $\mathrm{C}(a)$ は A の

[1] a is related to b の意味である.

部分集合であって $a \in \mathrm{C}(a)$ である. 集合族 $\{\mathrm{C}(a)\}_{a\in A}$ は集合 A を分割する[2] ことに注意しよう. 即ち次が成り立つ.

定理 1.2. a, b を集合 A の元とすれば次の 3 条件は互いに同値である.

1) $\mathrm{C}(a) = \mathrm{C}(b)$.

2) $\mathrm{C}(a)$ と $\mathrm{C}(b)$ は少なくとも一つの共通元を持つ.

3) $a\mathrm{R}b$ である.

証明. $\mathrm{C}(a)$ は空でない集合であるから自明に 1) から 2) が導かれる. 2) を仮定し $\mathrm{C}(a)$ と $\mathrm{C}(b)$ に共通な元 c を一つ取ると $c\mathrm{R}a$ かつ $c\mathrm{R}b$ が成り立つ. R は A 上の同値関係であったから $a\mathrm{R}c$ でもある. よって $a\mathrm{R}c$ かつ $c\mathrm{R}b$ より $a\mathrm{R}b$ となり 3) が得られた. 次に補題

(∗) a, b を A の元とする. このときもしも $a\mathrm{R}b$ ならば $\mathrm{C}(a)$ は $\mathrm{C}(b)$ の部分集合である.

を証明しよう. x を $\mathrm{C}(a)$ の元とすると, $x\mathrm{R}a$ かつ $a\mathrm{R}b$ であるから $x\mathrm{R}b$ となり, x は集合 $\mathrm{C}(b)$ の元であることが分かる. 従って $\mathrm{C}(a)$ は $\mathrm{C}(b)$ の部分集合である. さて, もしも $a\mathrm{R}b$ であれば, 上の補題 (∗) より $\mathrm{C}(a)$ は $\mathrm{C}(b)$ の部分集合であるが, 一方で $b\mathrm{R}a$ でもあるから補題 (∗) によって $\mathrm{C}(b)$ は $\mathrm{C}(a)$ の部分集合でもある. 即ち $a\mathrm{R}b$ ならば $\mathrm{C}(a) = \mathrm{C}(b)$ となり 3) から 1) が導かれる. □

例えば $A = \{x \mid x$ は整数で $1 \leqq x \leqq 31\}$ とし $\mathrm{R} = \{(a, b) \mid a, b \in A$ であって $a - b$ は 7 の倍数である $\}$ とすれば R は集合 A 上の同値関係であって, $\mathrm{C}(1) = \{1, 8, 15, 22, 29\}$, $\mathrm{C}(2) = \{2, 9, 16, 23, 30\}$, $\mathrm{C}(3) = \{3, 10, 17, 24, 31\}$, $\mathrm{C}(4) = \{4, 11, 18, 25\}$, $\mathrm{C}(5) = \{5, 12, 19, 26\}$, $\mathrm{C}(6) = \{6, 13, 20, 27\}$, $\mathrm{C}(7) = \{7, 14, 21, 28\}$. これをもう少し見易く書くと

C(1)	C(2)	C(3)	C(4)	C(5)	C(6)	C(7)
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

という表ができる. つまり 31 days 全体を一つの集合と考えてこれを a month と呼び, この集合を同値関係 R によって七つの同値類 C(1), C(2), C(3), C(4), C(5), C(6), C(7), に分け, これらの類をそれぞれ日曜日, 月曜日, 火曜日, 水曜日, 木曜日, 金曜日, 土曜日と呼んだものが, その月のカレンダーであると考えることができる. もとより $1 \neq 8$ であって $15 \neq 22$ であるが, これらは同じ曜日に属するという観点からはどれも日曜日であって, 日曜日であるという意味では区別をしない. このように同値関係によって集合を類別するという作業は, 同じ類 (単に類ともいう) に属する対象は (実際に違うものであっても) 同じものと見做し, 異なる対象をある観点から**同一視**しようとする

[2]空でない集合 A に対して集合族 $\mathcal{F}$ が A の分割であるとは, 次の 4 条件が満たされていることをいう： 1) $\mathcal{F}$ は A の部分集合の空でない集合であって, 2) $\mathcal{F}$ の元はどれも空集合でなく, 3) $\mathcal{F}$ の元の和集合は A に等しく, かつ, 4) C, C' が $\mathcal{F}$ の元で少なくとも一つ共通元を持てば実は $C = C'$ である.

高度に人間的な精神活動である. 集合 $A = \{1, 2, 3, 4\}$ に対して

$$\mathrm{R} = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (3,4), (4,3)\}$$

と置けば, R は A 上の同値関係である. $\mathrm{C}(1) = \{1, 2\}$, $\mathrm{C}(3) = \{3, 4\}$ であって R はこの集合 A を二つの類に分けている. この場合, 1 と 2 とは同じ類に属するから同一視され, 3 と 4 も同様に同値関係 R の観点からは同一視されるが, 1 と 3 とは違うものとして認識され同一視されることはない. 同一の集合を違った同値関係で類別すれば違った同一視が発生する. このようなものの考え方は数学的には平面上の図形の合同 (という同値関係) に抑もその由来があるのだろうが, この精神活動を人類の認識能力の発見の一つであると考えるならば, それは非常に古い (おそらくは何十万年もの) 歴史を持つに違いないと思われる.

定義 1.3. 集合 A 上の同値関係 R に対して同値類全体のなす集合 $A/\mathrm{R} := \{\mathrm{C}(a) \mid a \in A\}$ を A の R による**商集合**という. A の各元 a に対して $\mathrm{C}(a)$ を対応させる A から A/R への写像 $f : A \to A/\mathrm{R}$ を**自然な写像** (the canonical map) という.

各類の元をその類の**代表元** (a representative) という. 各類から元を一つずつ取ってこれらを全部集めてできた集合を商集合 A/R の**完全代表系** (a system of representatives) という. 完全代表系の取り方は一通りではない. 上のカレンダーの例で言えば, $\{1, 2, 3, 4, 5, 6, 7\}$ は一つの完全代表系であり, $\{8, 2, 17, 11, 5, 27, 28\}$ も一つの完全代表系である.

問 1.1 n を自然数とし複素数全体のなす集合を $\boldsymbol{C}$ とする. 集合 $A = \boldsymbol{C}^{n+1} - \{(0, 0, \ldots, 0)\}$ 上の関係 R を, $\mathrm{R} = \{(P, Q) \mid P, Q \in A$ であって $P = kQ$ となる $k \in \boldsymbol{C} - \{0\}$ が存在する $\}$ によって定義すれば, R は A 上の同値関係であることを証明せよ. 商集合 A/R を $\boldsymbol{C}$ **上の** $\boldsymbol{n}$ **次元射影空間**といい $\mathbf{P}^n(\boldsymbol{C})$ と書く.

問 1.2*[3] 有理数の Cauchy 列 $a = \{a_n\}_{n=1,2,\ldots}$ 全体よりなる集合を A とし A 上に関係 R を, $\mathrm{R} = \{(a, b) \mid a, b \in A$ であって, 数列 $\{a_n - b_n\}_{n=1,2,\ldots}$ は 0 に収束する $\}$ によって定義すれば, R は A 上の同値関係であることを証明せよ. また商集合 A/R から実数全体のなす集合 $\boldsymbol{R}$ への全単射 $h : A/\mathrm{R} \to \boldsymbol{R}$ で, A の全ての元 a について $h(\mathrm{C}(a)) = \lim a_n$ を満たすものが唯一つ存在することを証明せよ.

問 1.3 〜問 1.6 $A = \{1, 2, 3, 4\}$ とする. 次の集合 R は A 上の同値関係であるかどうか調べよ.

問 1.3^a $\mathrm{R} = \{(1,1), (2,2), (3,3), (4,4)\}$.

問 1.4^a $\mathrm{R} = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4), (2,1), (2,3), (2,4), (3,1), (3,2), (3,4), (4,1), (4,2), (4,3)\}$.

[3] * 印は高級であることを示す.

問 1.5^a　$\mathrm{R} = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,2),(3,2)\}$.

問 1.6^a　$\mathrm{R} = \{(1,1),(2,2),(3,3),(4,4),(2,3),(3,2),(2,4),(4,2),(3,4),(4,3)\}$.

問 1.7　n を自然数とし整数全体のなす集合を $\boldsymbol{Z}$ として

$$\mathrm{R}_n = \{(a,b) \mid a,b \in \boldsymbol{Z} \text{ であって } a-b \text{ は } n \text{ の倍数である } \}$$

と置く. 次の事実を確かめよ.

1)　R_n は集合 $\boldsymbol{Z}$ 上の同値関係である.

2)　商集合 $\boldsymbol{Z}/\mathrm{R}_n$ は n 個の元よりなる. (商集合 $\boldsymbol{Z}/\mathrm{R}_n$ の完全代表系を求めよ.)

3)　$r \in \boldsymbol{Z}$ とすれば $\mathrm{C}(r) = \{m \in \boldsymbol{Z} \mid m = nq + r\}$ である.

問 1.8*　A は空でない集合とする. 次の定理を証明せよ.

「集合を分割することと A 上に同値関係を定義することは同値である.」

問 1.9　集合 $A = \{1,2,3,4\}$ 上に同値関係を 10 通り定めよ.

問 1.10　A が無限集合であれば, A 上には無限に多くの同値関係が定義できることを示せ.

問 1.11*　V を $\boldsymbol{R}$ 上のベクトル空間として W をその部分空間とする. 次の事実を確かめよ.

1)　V 上の関係 R を, $\mathrm{R} = \{(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x},\boldsymbol{y} \in V \text{ であって } \boldsymbol{x}-\boldsymbol{y} \in W\}$ によって定義すれば, R は V 上の同値関係である.

2)　$\boldsymbol{x}$ を含む類 $\mathrm{C}(\boldsymbol{x}) \in V/\mathrm{R}$ を $\overline{\boldsymbol{x}}$ で表す. $\overline{\boldsymbol{x}}$ と $\overline{\boldsymbol{y}}$ の和 $\overline{\boldsymbol{x}}+\overline{\boldsymbol{y}}$ を $\overline{\boldsymbol{x}+\boldsymbol{y}}$ で定義する. この定義は矛盾なく定義されている (well-defined である) ことを示せ[4].

3)　$\alpha \in \boldsymbol{R}$ に対してスカラー倍 $\alpha\overline{\boldsymbol{x}}$ を $\overline{\alpha\boldsymbol{x}}$ で定義する. この定義は well-defined であることを示せ[5].

4)　上の和とスカラー倍によって V/R は $\boldsymbol{R}$ 上のベクトル空間になることを示せ[6]. このベクトル空間を V の W による**商空間**と呼び V/W で表す.

§2　写像 (maps)

まず写像の定義を復習しよう.

定義 2.1(the formal definition of maps).　A, B は空でない集合とし, f は直積集合 $A \times B$ の部分集合とせよ. 次の 2 条件を満たすとき f は集合 A から B 集合への**写像** (a map) であるという.

---

[4] $\boldsymbol{x}\mathrm{R}\boldsymbol{x}_1$, $\boldsymbol{y}\mathrm{R}\boldsymbol{y}_1$ であるとき, $\overline{\boldsymbol{x}} = \overline{\boldsymbol{x}_1}$, $\overline{\boldsymbol{y}} = \overline{\boldsymbol{y}_1}$ であるから, $\overline{\boldsymbol{x}}+\overline{\boldsymbol{y}} = \overline{\boldsymbol{x}_1}+\overline{\boldsymbol{y}_1}$ が成り立たなければこの定義は意味をなさない. ここで言っている意味は, $\boldsymbol{x}\mathrm{R}\boldsymbol{x}_1$, $\boldsymbol{y}\mathrm{R}\boldsymbol{y}_1$ ならば $\overline{\boldsymbol{x}}+\overline{\boldsymbol{y}} = \overline{\boldsymbol{x}_1}+\overline{\boldsymbol{y}_1}$ であることを示せということ.

[5] $\boldsymbol{x}\mathrm{R}\boldsymbol{x}_1$ であれば $\alpha\overline{\boldsymbol{x}} = \alpha\overline{\boldsymbol{x}_1}$ であることを示せという意味.

[6] ベクトル空間の公理を全て証明するのは大変なので, $\alpha(\overline{\boldsymbol{x}}+\overline{\boldsymbol{y}}) = \alpha\overline{\boldsymbol{x}}+\alpha\overline{\boldsymbol{y}}$ 及び $\alpha(\beta\overline{\boldsymbol{x}}) = (\alpha\beta)\overline{\boldsymbol{x}}$ のみ示せ.

1)　a を A の元とすれば, この a に対して (a,b) が f の元となるような元 b が少なくとも一つは B 内に含まれている.
2)　a は A の元で b, b' は B の元とする. もしも (a,b) と (a,b') が両方とも f の元であれば必ず $b=b'$ が成り立つ.

この定義は「写像とは A の各元に対して一つずつ B の元を対応させる規則のことである.」という使い易い定義を, 念のために数学的に厳密に述べたものに過ぎない. f が集合 A から集合 B への写像であることを $f:A\to B$ と書く. このとき A の元 a を一つ与える毎に, (a,b) が f の元となるような B の元 b が唯一つ定まる. 元 a に対して定まるこの b を $f(a)$ と書き, **f による a の像** (the image of a) という. 例えば $A=\{1,2,3,4,5,6,7\}$, $B=\{1,2,3\}$ のときに

$$f=\{(1,1),(2,2),(3,3),(4,1),(5,2),(6,3),(7,1)\}$$

と置けば, f は集合 A から集合 B への一つの写像であって, $f(1)=1$, $f(2)=2$, $f(3)=3$, $f(4)=1$, $f(5)=2$, $f(6)=3$, $f(7)=1$ である. 対応として見れば

$$f=\begin{bmatrix}1&2&3&4&5&6&7\\1&2&3&1&2&3&1\end{bmatrix}$$

となる[7].

二つの写像 $f:A\to B$ と $g:C\to D$ とは, $A=C$, $B=D$ であってかつ等式 $f(a)=g(a)$ が A の全ての元 a に対して成り立つとき, 同じものであると考え $f=g$ と書く. 写像 $g:A\to B$ と $f:B\to C$ とが与えられているとき, A の元 a に対して $h(a)=f(g(a))$ と定めると集合 A から集合 B への写像 $h:A\to C$ が得られる. この h のことを **f と g の合成**と言って $f\circ g$ (又は単に fg) と書く. 即ち

$$(f\circ g)(a)=f(g(a))$$

である.

定義 2.2.　写像 $f:A\to B$ がある.
1)　A の元 a, a' について $f(a)=f(a')$ ならば必ず $a=a'$ が成り立つとき, f は**一対一写像** (one-to-one) (又は単射) であるという.
2)　b が B の元であれば $b=f(a)$ となる A の元 a が少なくとも一つ存在するとき, f は**上への写像** (onto) (又は全射) であるという.
3)　一対一かつ上への写像であるとき f は**全単射**であるという.

空でない二つの集合 A, B の間に全単射 $f:A\to B$ が存在すれば, この写像 f を用いて A, B には全く同じ数学的構造を入れることができる. 全単射の存在は極めて重要である.

[7]後に出てくる置換の記法を真似してこの様に書いたが, 一般的な書き方ではない.

$f : A \to B$ は全単射とする. このとき b を B の元とすると $b = f(a)$ となるような A の元 a が一つだけ存在する. 従って $g(b) = a$ とすれば g は B から A への写像となる. この写像 $g : B \to A$ を **f の逆写像**と言って f^{-1} と書き $\underline{f\text{-inverse}}$ と読む.

例えば $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{7, 8, 9, 10, 11, 12\}$ とし $f : A \to B$ を

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 11 & 9 & 12 & 7 & 10 & 8 \end{bmatrix}$$

とすれば, f は全単射であって

$$\begin{aligned} f^{-1} &= \begin{bmatrix} 11 & 9 & 12 & 7 & 10 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{bmatrix} \end{aligned}$$

である. このとき

$$\begin{aligned} f^{-1} \circ f &= \begin{bmatrix} 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 11 & 9 & 12 & 7 & 10 & 8 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \\ f \circ f^{-1} &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 11 & 9 & 12 & 7 & 10 & 8 \end{bmatrix} \circ \begin{bmatrix} 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 8 & 9 & 10 & 11 & 12 \end{bmatrix} \end{aligned}$$

であるから $f^{-1} \circ f = 1_A$ と $f \circ f^{-1} = 1_B$ を得る. (但し空でない集合 X に対して 1_X は X 上の恒等写像 $1_X : X \to X$, $1_X(x) = x$ を表す.) また f^{-1} も全単射である.

一般に次が正しい.

補題 2.3. $f : A \to B$ は全単射とする. このとき

1) $f^{-1} \circ f = 1_A$ であって $f \circ f^{-1} = 1_B$ である. 但し空でない集合 X に対して 1_X は X 上の恒等写像 $1_X : X \to X$, $1_X(x) = x$ を表す.

2) f^{-1} も全単射である.

3) $(f^{-1})^{-1} = f$ である.

証明. 1) $f^{-1} \circ f$ も 1_A も集合 A から A 自身への写像であって $1_A(a) = a$ であるから, $(f^{-1} \circ f)(a) = a$ が全ての $a \in A$ について成り立つことを示せばよい. 合成写像の定義より $(f^{-1} \circ f)(a) = f^{-1}(f(a))$ であり, 写像 f^{-1} の定義より $(f^{-1}(f(a)) = a$. よって $(f^{-1} \circ f)(a) = a$. 故に $f^{-1} \circ f = 1_A$. 次に $f \circ f^{-1} = 1_B$ であることを確かめよう. $f \circ f^{-1}$ も 1_B も集合 B から B 自身への写像であって $1_B(b) = b$ であるから, $(f \circ f^{-1}) = b$ が全ての $b \in B$ について成り立つことを示せばよい. 合成写像の定義より $(f \circ f^{-1})(b) = f(f^{-1}(b))$ であり, 写像 f^{-1} の定義より $f(f^{-1}(b)) = b$. 故に $(f \circ f^{-1})(b) = b$. 従って $f \circ f^{-1} = 1_B$.

2) は問 2.19 及び問 2.20 による.

3) は定義に従う. □

定義 2.4. 写像 $f : A \to B$ に対して $\mathrm{R}_f = \{(a, b) \mid a, b \in A$ であって $f(a) = f(b)$ である $\}$ と置く. R_f は集合 A 上の同値関係である.

A の各元 a に対して $\mathrm{C}(a)$ を対応させる自然な写像 $f : A \to A/\mathrm{R}$, $f(a) = \mathrm{C}(a)$ については, 定理 1.2 より $\mathrm{R}_f = \mathrm{R}$ が成立する.

定理 2.5. R は空でない集合 A 上の同値関係とする. 集合 A から商集合 A/R への自然な写像を f とする. このとき

1) a, b が A の元ならば, $a\mathrm{R}b \iff f(a) = f(b)$.

2) 写像 $g : A \to B$ は条件

$$(*)\ \underline{a, b \text{ が } A \text{ の元で } a\mathrm{R}b \text{ ならば } g(a) = g(b) \text{ である}}$$

を満たすと仮定せよ. このとき商集合 A/R から集合 B への写像 $h : A/\mathrm{R} \to B$ で $g = h \circ f$ となるものが唯一つ存在する.

3) 写像 $g : A \to B$ は条件 $(*)$ を満たすと仮定し, 写像 $h : A/\mathrm{R} \to B$ を $g = h \circ f$ となるように取る. このとき h が単射であるための必要十分条件は $\mathrm{R} = \mathrm{R}_g$ が成り立つことである.

解説 2.6. 上の定理は抽象的で少々理解しづらい所があるかも知れない. この様な場合には常に例で理解するように心がけると良い. A を人間全体の集合として, $\mathrm{R} = \{(a, b) \in A \times A \mid a, b$ は同じ国の国民である $\}$ とする[8]. このとき, A/R は全ての人間を同国人同士でまとめたものであるから, $A/\mathrm{R} =$ { 日本人, 米国人, 韓国人, 北朝鮮人[9], $\cdots$ } と見做せ, f(森喜朗) = 日本人, f(ブッシュ) = 米国人, f(金大中) = 韓国人 である. B を料理全体の集合とする[10]. 写像 $g : A \to B$ をある日の夕食に食べる料理を対応させる写像とする[11]. 条件 $(*)$ は同国人は同じ料理を食べることを意味するから, g(森喜朗) = 刺身, g(ブッシュ) = ハンバーガー, g(金大中) = 焼肉 であれば, h(日本人) = 刺身, h(米国人) = ハンバーガー, h(韓国人) = 焼肉 を満たす写像 $h : A/\mathrm{R} \to B$ が存在して $g = h \circ f$ となる. g が $(*)$ を満たしても, g(金正日) = 焼肉 であれば h(北朝鮮人) = 焼肉[12] となって h は単射ではない. このとき (金大中, 金正日) $\notin \mathrm{R}$ であるが, (金大中, 金正日) $\in \mathrm{R}_g$ より $\mathrm{R} \subsetneq \mathrm{R}_g$ である.

定理 2.5 の証明 1) は定理 1.2 による.

2) を考えよう. A/R の元を任意に一つ取りこれを C とする. C は同値類であるから $\mathrm{C} = \mathrm{C}(a_0)$ となる A の元 a_0 (即ち類 C の代表元) が少なくとも一つは存在するが, $\mathrm{C} = \mathrm{C}(a)$ となる A の元 a は C に対してこの a_0 一つしかない訳ではなく, $a_0\mathrm{R}a$ なるいかなる元 $a \in A$ も等式 $\mathrm{C} = \mathrm{C}(a)$ を満たす (定理 1.2 を見よ). しかしながら $\mathrm{C} = \mathrm{C}(a)$ であれば定理 1.2 より $a_0\mathrm{R}a$ であり, 仮定した条件 $(*)$ によれば $a_0\mathrm{R}a$ であるいかなる a についても $g(a_0) = g(a)$ が成り立つ. 即ち固定された同値類

[8] 全ての人間は唯一の国籍を持つと仮定する.
[9] 所属する国で分類していて民族で分類している訳ではないので, 韓国人と北朝鮮人は区別される.
[10] 料理全体が集合をなすことを仮定する.
[11] 人間 a が天麩羅と刺身を食べると, $g(a) =$ { 天麩羅, 刺身 } となって g が写像でなくなるので, 料理を一種類しか食べないと仮定する.
[12] 北朝鮮の国民全員が焼き肉を食べられるか否かはこの際問題にしない.

C に対して $\mathrm{C} = \mathrm{C}(a)$ となるどんな元 $a \in A$ を選ぼうと, $g(a)$ の値は a の取り方にはよらず共通である. よって $h(\mathrm{C}) = g(a_0)$ と定めることによって, 集合 A/R から集合 B への写像 $h : A/\mathrm{R} \to B$ が得られる. 勿論 a を A の元とすれば $h(\mathrm{C}(a)) = g(a)$ である. 従って $g = h \circ f$. 次に商集合 A/R から集合 B への写像 $h' : A/\mathrm{R} \to B$ が $g = h' \circ f$ を満たすと仮定し $h' = h$ であることを確かめよう. C を集合 A/R の任意の元としこれを $\mathrm{C} = \mathrm{C}(a_0)$ と書く. すると $h'(\mathrm{C}) = h'(\mathrm{C}(a_0)) = g(a_0)$ であって, $h(\mathrm{C}) = h(\mathrm{C}(a_0)) = g(a_0)$ であるから, $h'(\mathrm{C}) = h(\mathrm{C})$ を得る. 故に $h' = h$ である. 即ち商集合 A/R から集合 B への写像 $h : A/\mathrm{R} \to B$ で $g = h \circ f$ を満たすものは上に定めた h のみである.

3) を証明しよう. $\mathrm{R}_g = \{(a, b) \mid a, b \in A$ であって $g(a) = g(b)$ である $\}$ であった. 条件 $(*)$ は R が R_g の部分集合であることを意味する. さて (a, b) を R_g の任意の元とすると, $g(a) = g(b)$ であるから $h(\mathrm{C}(a)) = h(\mathrm{C}(b))$, よってもし h が単射であれば $\mathrm{C}(a) = \mathrm{C}(b)$. 定理 1.2 より $a\mathrm{R}b$, 即ち (a, b) は R の元である. 故に h が単射であれば R_g は R の部分集合となり $\mathrm{R} = \mathrm{R}_g$ を得る. 逆に $\mathrm{R} = \mathrm{R}_g$ と仮定しよう. A/R の二つの元 C, D を取り $\mathrm{C} = \mathrm{C}(a)$, $\mathrm{D} = \mathrm{C}(b)$ $(a, b \in A)$ と書く. もし $h(\mathrm{C}) = h(\mathrm{D})$ であれば $g(a) = g(b)$ であるから (a, b) は R_g の元であって, 仮定より (a, b) は R の元である. 故に定理 1.2 より $\mathrm{C}(a) = \mathrm{C}(b)$ となり $\mathrm{C} = \mathrm{D}$ を得る. 従って h は単射である. よって h が単射であるための必要十分条件は $\mathrm{R} = \mathrm{R}_g$ が成り立つことである. □

次の系は商集合の構成によらない定義[13] である.

系 2.7. R は空でない集合 A 上の同値関係とする. 全射 $g : A \to B$ が $\mathrm{R}_g = \mathrm{R}$ を満たすならば, 商集合 A/R から集合 B への全単射 $h : A/\mathrm{R} \to B$ で $g = h \circ f$ となるものが唯一つ存在する.

証明. 定理 2.5 の 2) によって商集合 A/R から集合 B への写像 $h : A/\mathrm{R} \to B$ で $g = h \circ f$ となるものが唯一つ存在する. g が全射であるから, 問 2.20 より h は全射である. 定理 2.5 の 3) より h は単射でもある. □

問 2.1 $A = \{1, 2, 3, 4, 5, 6, 7\}$, $B = \{1, 2, 3\}$ とする. $g = \{(2, 2), (3, 3), (4, 1), (5, 2), (6, 3), (7, 1)\}$ は集合 A から集合 B への写像ではない. $h = \{(1, 1), (1, 2), (2, 3), (3, 3), (4, 1), (5, 2), (6, 3), (7, 1)\}$ も集合 A から集合 B への写像ではない. 理由を述べよ.

問 2.2 〜問 2.6 $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3, 4, 5, 6\}$, $C = \{1, 2, 3, 4\}$ とし, $g : A \to B$, $f : B \to C$ とする. 次の写像 f, g を合成せよ.

問 2.2^b $\quad f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 3 & 4 \end{bmatrix}$, $\quad g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 6 & 1 \end{bmatrix}$.

問 2.3^b $\quad f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 2 & 4 \end{bmatrix}$, $\quad g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 5 & 4 & 1 \end{bmatrix}$.

[13]「圏論的特徴付け」と呼ばれる.

問 2.4^b $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 4 & 3 & 3 & 3 & 1 \end{bmatrix}$, $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 5 & 4 & 2 & 3 \end{bmatrix}$.

問 2.5^b $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 1 & 2 & 3 & 4 & 4 \end{bmatrix}$, $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 6 & 1 \end{bmatrix}$.

問 2.6^b $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 2 & 1 \end{bmatrix}$, $g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 6 & 1 \end{bmatrix}$.

問 2.7 $A = \{1,2,3,4,5\}$, $B = \{1,2,3,4,5,6\}$, $C = \{1,2,3,4\}$ とし, A から B への単射を 3 個, B から C への全射を 3 個作ってこれらを合成せよ.

問 2.8 〜問 2.15 次の写像は単射であるか, 全射であるか, あるいは全単射であるか調べよ.

問 2.8^c $f : \boldsymbol{R} \to \boldsymbol{R}$, $f(x) = x + 1$.

問 2.9^c $f : \boldsymbol{R} \to \boldsymbol{R}$, $f(x) = x^2$.

問 2.10^c $f : \boldsymbol{N} \to \boldsymbol{N}$, $f(n) = n^2$. 但し $\boldsymbol{N}$ は自然数全体のなす集合を表す.

問 2.11^c $f : \boldsymbol{R} \to \boldsymbol{R}^+$, $f(x) = \exp(x)$. 但し $\boldsymbol{R}^+$ は正の実数全体のなす集合を表す.

問 2.12^c $f : \boldsymbol{N} \to \boldsymbol{N}$, $f(1) = 1$ で $n \geqq 2$ なら $f(n) = n - 1$.

問 2.13^c $f : \boldsymbol{R} \to M_2(\boldsymbol{R})$, $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. 但し $M_n(\boldsymbol{R})$ は n 次の実正方行列全体のなす集合を表す.

問 2.14^c 行列 $\begin{pmatrix} 2 & -1 & 5 \\ 3 & 1 & 1 \end{pmatrix}$ の定める線形写像 $f : \boldsymbol{R}^3 \to \boldsymbol{R}^2$.

問 2.15^c $f : M_n(\boldsymbol{R}) \to \boldsymbol{R}$, $f(A) = \det A$.

問 2.16^d 単射を二つ合成すればやはり単射が得られる[14].

問 2.17^d 全射を二つ合成すればやはり全射が得られる.

問 2.18^d 全単射を二つ合成すればやはり全単射が得られる.

問 2.19^d $g : A \to B$ と $f : B \to C$ の合成 $f \circ g$ が単射であれば g は単射である.

問 2.20^d $g : A \to B$ と $f : B \to C$ の合成 $f \circ g$ が全射であれば f は全射である.

§3 演算 (binary operations)

この節では常に G は空でない集合を表すことにする. 直積集合 $G \times G$ から集合 G への写像 $m : G \times G \to G$ を集合 G 上の**演算** (a binary operation on G) という. G 上の演算 m が予め一つ指定されているときは, G の元 a, b に対して組 (a,b) の m による像 $m((a,b))$ を単に ab (又は $a \cdot b$, $a \circ b$, $a * b$ 等どんな記号を使ってもよいけれど) と書き, これを <u>a カケル b</u> と読み ***a* と *b* の積**と呼ぶことにする. G 上の二つの演算 m, m' は $G \times G$ から G への写像として等しいとき, 即ち全ての組 (a,b) に対して等号 $m((a,b)) = m'((a,b))$ が成り立つとき $m = m'$ であると考える.

[14]「ことを証明せよ」を省略している. 以下同様.

例 3.1. $G = \{1, 2, 3\}$ とする. このとき $G \times G = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$ である. G 上に演算を一つ定めることは, $G \times G$ の以上の 9 個の元に対して G の元を一つずつ対応させる規則を定めることに他ならない. 例えば $(1,1)$ には 1 を, $(1,2)$ には 2 を, $(1,3)$ には 3 を, $(2,1)$ には 2 を, $(2,2)$ には 3 を, $(2,3)$ には 1 を, $(3,1)$ には 3 を, $(3,2)$ には 1 を, $(3,3)$ には 2 を対応させ, この対応 (即ち $G \times G$ から G への写像) を m と呼ぶことにすれば, m は G 上の一つの演算である. G の元 a, b に対して組 (a, b) の m による像 $m((a, b))$ を $a \cdot b$ と書くことにしたのであるから, この例では

$$1 \cdot 1 = 1, \quad 1 \cdot 2 = 2, \quad 1 \cdot 3 = 3,$$
$$2 \cdot 1 = 2, \quad 2 \cdot 2 = 3, \quad 2 \cdot 3 = 1,$$
$$3 \cdot 1 = 3, \quad 3 \cdot 2 = 1, \quad 3 \cdot 3 = 2$$

である.

以上の考え方をもっと簡略化すると, G 上に演算を定めることは, 次の表

	1	2	3
1	○	○	○
2	○	○	○
3	○	○	○

の 9 個の “○”の全てを G の元で置き換えることに他ならない. 上の例では

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

である. また

	1	2	3
1	1	1	1
2	1	1	1
3	1	1	1

としても立派に G 上に一つの演算 m' を定めたことになる. G 上の二つの演算 m, m' は $G \times G \to G$ から G への写像として等しいとき同じものであると考えるのであるから, 上の例では $m \neq m'$ である. 9 個の “○”を 3 つの数で置き換えるのであるから, この G 上には全部で $3^9 = 19683$ 個の演算があることになる. 但しこれら全てに価値がある訳ではなく, 数学的に意味のある演算は実は少ない. 例えば, 後に確かめるが, その演算に関して G が群になるものは (順序の違いを除いて) たった一つである.

例 3.2. 普通の数の和と積は勿論集合 $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ 上の演算である. 但し $\boldsymbol{Q}$ は有理数全体のなす集合を表す. ベクトルの和は集合 $\boldsymbol{R}^n$ 上の演算である. 行列の和は勿論集合 $M_{m,n}(\boldsymbol{R})$ 上の演算である. ここで $M_{m,n}(\boldsymbol{R})$ は (m,n) 型の実行列全体のなす集合を表す. 行列の積は $M_n(\boldsymbol{R})$ 上の演算である. このように演算の例は極めて多彩である.

以下この節では集合 G 上には演算が一つ与えられているものと仮定する.

定義 3.3. e は G の元とする. 全ての G の元 a に対して等号 $ae = ea = a$ が成り立つとき, e は G の**単位元** (an identity element of G) であるという.

例 3.4. $G = \{1,2,3\}$ とし G に演算 m を次の表 1) によって定めると $e = 1$ は G の単位元である. また表 2) によって定めても立派に G 上の演算であるが, この演算 m' に関しては集合 G は単位元を持たない.

1)

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

2)

	1	2	3
1	1	1	1
2	2	2	2
3	3	3	3

例 3.5. 普通の数の和を集合 $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ 上の演算と見なせば, 数 0 が単位元である. ベクトルの和を集合 $\boldsymbol{R}^n$ 上の演算と見れば零ベクトル $\boldsymbol{o}$ が単位元である. 行列の和は集合 $M_{m,n}(\boldsymbol{R})$ 上の演算であり零行列が単位元となっている. 行列の積は $M_n(\boldsymbol{R})$ 上の演算であって単位行列 E が単位元である.

補題 3.6. 仮に集合 G が単位元を持ったとしても, その単位元は唯一である.

証明. e, e' がどちらも G の単位元であったと仮定する. このとき定義より G の全ての元 a に対して等式 $ae = ea = a$ と等式 $ae' = e'a = a$ とが成り立つ. a は G の任意の元であるから, はじめの等式において $a = e'$ とすれば $ee' = e'$ であって, 二番目の等式で $a = e$ とすれば $ee' = e$. 故に $e = e'$ である. 即ち G 内には単位元は唯一つしか含まれていないことが分かる. □

定義 3.7. 空でない二つの集合 G, G' にそれぞれ演算が与えられていると仮定せよ. 写像 $f : G \to G'$ は次の条件

$$\underline{G \text{ の全ての元 } a, b \text{ について } f(ab) = f(a)f(b) \text{ となる}}$$

を満たすとき, **準同型写像** (a homomorphism) であるという. 勿論この条件で ab は a と b の G 内での積を表し, $f(a)f(b)$ は G' 内での $f(a)$ と $f(b)$ の積を表す.

例えば $G = \{1,2,3\}$, $G' = \{4,5,6,7\}$ とし G, G' 上の演算を次の表

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

,

	4	5	6	7
4	4	5	6	7
5	5	5	6	7
6	6	6	7	5
7	7	7	5	6

で定義し写像 $f : G \to G'$ を $f(1) = 5$, $f(2) = 6$, $f(3) = 7$ とすると f は準同型である. 実際 G' 内で $5 = f(1)$, $6 = f(2)$, $7 = f(3)$ の積の表を作ると

	5	6	7
5	5	6	7
6	6	7	5
7	7	5	6

$=$

	$f(1)$	$f(2)$	$f(3)$
$f(1)$	$f(1)$	$f(2)$	$f(3)$
$f(2)$	$f(2)$	$f(3)$	$f(1)$
$f(3)$	$f(3)$	$f(1)$	$f(2)$

であって, これは G の積の表

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

の数を f で移したものに他ならない. 従って $f(ab) = f(a)f(b)$ が G の全ての元 a, b について成り立つ.

$G = \boldsymbol{R}$, $G' = \{a \in \boldsymbol{R} \mid a > 0\}$ とし写像 $f : G \to G'$ を $f(x) = \exp(x)$ と定めると f は準同型写像である. 勿論ここで G の演算は数の加法を G' の演算は数の乗法を採用している.

定義 3.8. 空でない二つの集合 G, G' にそれぞれ演算が与えられていると仮定せよ.

1) 準同型写像 $f : G \to G'$ は全単射であるとき, **同型写像** (an isomorphism) であるという.

2) G から G' への同型写像が少なくとも一つ存在するとき G と G' とは互いに**同型** (isomorphic) であるという.

$G = \boldsymbol{R}$, $G' = \{a \in \boldsymbol{R} \mid a > 0\}$ とし, 写像 $f : G \to G'$ を $f(x) = \exp(x)$ と定めると f は同型写像であるから G と G' は同型である. しかし $G'' = \{a \in \boldsymbol{R} \mid a \neq 0\}$ とおき G'' の演算として数の乗法を採用することにすると, G と G'' とは同型ではない. 実際もしも G と G'' とが同型であるならば, 定義により同型写像 $f : G \to G''$ を少なくとも一つはとれる. すると f は準同型であるから $f(a) = f((a/2) + (a/2)) = f(a/2) \times f(a/2) = f(a/2)^2$ が成り立つ. 従って全ての $a \in G$ について $f(a) \geqq 0$ となるので f は全射ではない. よって G と G'' とは同型でない. 後に G, G', G'' はいずれも群になることを確かめるが, 上の議論は G と G' は群としては数学的に同じものであるが, G と G'' とは本質的に異なることを示していると考えられる.

問 3.1 集合上 $G_1 = \{1\}$, $G_2 = \{1, 2\}$, $G_3 = \{1, 2, 3\}$, $G_4 = \{1, 2, 3, 4\}$, $G_6 = \{1, 2, 3, 4, 5\}$,

$G_6 = \{1, 2, 3, 4, 5, 6\}$ に演算を一つずつ定めよ.

問 3.2　整数全体からなる集合 $\boldsymbol{Z}$ 上に演算を $a * b = ab + a + b$ によって定めるとき,

1)　$(a * b) * c = a * (b * c)$ が全ての a, b, $c \in \boldsymbol{Z}$ について成り立つことを示せ.

2)　$a * b = b * a$ が全ての a, $b \in \boldsymbol{Z}$ について成り立つことを示せ.

問 3.3　集合 G_1, G_2, $\cdots$, G_n 上に演算が与えられているとき

$$(a_1, a_2, \cdots, a_n) \circ (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

と定めれば, この $\circ$ は直積集合 $G = G_1 \times G_2 \times \cdots \times G_n$ 上の演算であることを確かめよ.

問 3.4　問 3.2 の演算は単位元を持つことを示せ.

問 3.5　問 3.3 において全ての G_i $(i = 1, 2, \cdots, n)$ が単位元を持てば G も単位元を持つことを示せ.

問 3.6　空でない二つの集合 G, G' にそれぞれ演算が与えられていると仮定し, $f : G \to G'$ は準同型写像で全射であると仮定せよ. このときもし G が単位元を持てば G' も単位元を持つことを示せ.

問 3.7　空でない三つの集合 G, G', G'' にそれぞれ演算が与えられていると仮定し, $g : G \to G'$, $f : G' \to G''$ をそれぞれ準同型写像とする. 次の主張を証明せよ.

1)　合成写像 $f \circ g : G \to G''$ も準同型写像である.

2)　もしも f, g が両方とも同型写像であれば $f \circ g$ も同型写像である.

3)*　g が同型写像であれば g の逆写像 $g^{-1} : G' \to G$ も同型写像である.

問 3.8　問 3.3 において集合 G から集合 G_i への写像 $p_i : G \to G_i$, $p_i((a_1, a_2, \cdots, a_n)) = a_i$ は全ての i について準同型で全射であることを確かめよ.

§4　半群 (semigroups)

G は空でない集合であって, かつ G 上には演算が一つ与えられていると仮定する.

定義 4.1.

1)　全ての G の元 a, b, c に対して等式 $(ab)c = a(bc)$ が成り立つとき G は**結合法則**を満たすという.

2)　全ての G の元 a, b に対して等式 $ab = ba$ が成り立つとき G は**交換法則**を満たすという.

定義 4.2.　単位元 e を持ちかつ結合法則を満たすとき G は**半群** (a semigroup) であるという.

例えば自然数の全体よりなる集合 $\boldsymbol{N}$ は数の乗法を演算として半群をなす. また $\boldsymbol{N} \cup \{0\}$ は数の加法を演算として半群となる. これらは最も基本的な半群である. $M_n(\boldsymbol{R})$ は行列の積を演算として半群をなし, n 次の単位行列 E が単位元となる. 半群の例もまた多彩である.

定義 4.3. G は単位元 e を持つと仮定する. a を G の元とする. 等式 $ax = xa = e$ を満たす元 x が G 内に少なくとも一つ存在するとき, 元 a は**逆元** (an inverse) を持つという.

$G = M_n(\boldsymbol{R})$ は行列の積を演算にして半群となり, 単位行列 E が単位元であった. A を $M_n(\boldsymbol{R})$ の元とするとき, A が $M_n(\boldsymbol{R})$ 内に逆元を持つことと, 行列 A が逆行列をも (つつまり正則である) こととは同値である.

$G = \{1, 2, 3\}$ とし集合 G 上に演算を次の表

	1	2	3
1	1	2	3
2	2	1	1
3	3	1	2

によって定めると $e = 1$ は G の単位元である. 2 と 3 は 2 の逆元である. この例によって分かるように逆元は必ずしも一意的には定まらない. しかし

命題 4.4. G は半群であるとき, G の元 a が逆元を持つならばそれは唯一つである.

証明. x, y を a の逆元とすれば, 等式 $ax = xa = e$ と $ay = ya = e$ とが成り立つ. よって $x = ex = (ya)x = y(ax) = ye = y$ である. □

逆行列の記号と同じ記号を用いて

定義 4.5. G は半群であるとする. G の元 a が逆元を持つとき, a の逆元を a^{-1} と書き $\underline{a}$-inverse と読む.

例題 4.6. X を空でない集合とし X から X への写像全体のなす集合を M_X とすれば, M_X は写像の合成を演算にして半群になる. M_X の単位元は 1_X である.

証明. $M_X = \{f \mid f : X \to X$ は写像である $\}$ である. $1_X \in M_X$ であるから M_X は空集合ではない. f, g を M_X の元とすれば, 写像 f と g の合成写像 $f \circ g$ はやはり M_X の元である. 従って写像の合成によって集合 M_X 上に演算が得られる. この演算について M_X は半群となることを確かめよう. $e = 1_X$ と置き f を M_X の元とすれば, 任意の $x \in X$ に対して $(ef)(x) = e(f(x)) = f(x)$ であって $(fe)(x) = f(e(x)) = x$. 従って $ef = fe = f$. 即ち e は M_X の単位元である. f, g, h を M_X の元とすると, 任意の $x \in X$ に対して $((fg)h)(x) = (fg)(h(x)) = f(g(h(x)))$. 一方 $(f(gh))(x) = f((gh)(x)) = f(g(h(x)))$. よって $((fg)h)(x) = f(g(h(x))) = (f(gh))(x)$. 故に $(fg)h = f(gh)$. 即ち M_X は半群である. □

系 4.7. f を M_X の元とすると次の二つの条件は同値である.

1) f が M_X 内に逆元を持つ.

2) f は全単射である.

このとき f の逆写像が M_X 内での f の逆元になっている.

証明. f が M_X 内に逆元を持つならばその逆元を g とすると, 逆元の定義により等式 $fg = gf = e$ が成り立つ. ここで M_X の単位元 $e = 1_X$ はであって 1_X は全単射であるから, 問 2.19 と問 2.20 より f も全単射である. 逆に f は全単射であると仮定しよう. すると f は逆写像を持つから f の逆写像を g と書くと, 補題 2.3 より $fg = gf = 1_X$ $(= e)$ が成り立つ. 勿論 g は M_X の元であるから g は M_X 内での f の逆元である. □

問 4.1 $G = \{0, 1, 2\}$ とし G 上に演算を次の表によって定めると半群ができることを確かめよ.

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

問 4.2 $G = \{(a, b) \in \boldsymbol{R}^2 \mid a \neq 0\}$ とし集合 G 上の演算を

$$(a, b) \cdot (c, d) = (ac, bc + d)$$

によって定めると G は半群になることを確かめよ.

問 4.3 集合 G_1, G_2, $\cdots$, G_n が半群であれば, 直積集合 $G = G_1 \times G_2 \times \cdots \times G_n$ も演算 $(a_1, a_2, \cdots, a_n) \circ (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$ によって半群となることを示せ.

問 4.4 〜 4.9 次の集合 G は指定された演算に関して単位元を持つか, 結合法則を満たすか, 交換法則を満たすか, 半群になるかを調べよ. 単位元を持つ場合には, G の元について逆元を持つかどうかも調べよ.

問 4.4^e $G = \boldsymbol{Q}$, $a \cdot b = (a + b)/3$.

問 4.5^e $G = \boldsymbol{Z}$, $a \cdot b = a + b - 1$.

問 4.6^e $G = \boldsymbol{R}$, $a \cdot b = ab + a + b$.

問 4.7^e $G = \{1, 2, 3\}$,

	1	2	3
1	2	3	1
2	3	2	2
3	1	2	3

.

問 4.8^e $G = \{0, 1, 2, 3\}$,

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.

問 4.9^{e}　$G = \{f \mid f$ は $\boldsymbol{R}$ から $\boldsymbol{R}$ への写像である $\}$, $(f \cdot g)(x) = f(x)g(x)$, $(f + g)(x) = f(x) + g(x)$.

問 4.10*　$X = \boldsymbol{R} - \{0, 1\}$ とし G は次の 6 個の写像 e, a, b, c, f, g よりなる M_X の部分集合で演算は写像の合成とする. $e(x) = x$, $a(x) = 1 - x$, $b(x) = 1/x$, $c(x) = x/(x-1)$, $f(x) = (x-1)/x$, $g(x) = 1/(1-x)$. 下の表を完成せよ.

	e	a	b	c	f	g
e	e	a	b	c	f	g
a		e				
b			e			
c				e		
f						e
g					e	

問 4.11　$X = \{1, 2, 3\}$ とする. §2 で使った書き方で M_X の元を表そう. 即ち $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \end{bmatrix}$ とは 1, 2, 3 をそれぞれ 1, 3, 1 に対応させる写像である. この記述の仕方で, 半群 M_X の元を全て書き出し, その中で逆元を持つものを指摘しその逆元を求めよ.

問 4.12 〜問 4.16　G は半群とする. 次の主張を証明せよ.

問 4.12^{f}　G の単位元 e は必ず逆元を持ち, $e^{-1} = e$ が成り立つ.

問 4.13^{f}　G の元 a が逆元を持てば, a^{-1} も逆元を持ち等式 $(a^{-1})^{-1} = a$ が成り立つ.

問 4.14^{f}　a, x, y は G の元とし, a は逆元を持つと仮定する. このとき $ax = ay$ であれば $x = y$ である. また $xa = ya$ であれば $x = y$ である.

問 4.15^{f}　G の元 a が逆元を持ち, かつ $aa = a$ であれば $a = e$ である.

問 4.16^{f}　G の元 a, b が逆元を持てば, 積 ab も逆元を持ち $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ.

問 4.17 〜問 4.19　G は半群とする. G の元 a に対して写像 $L_a : G \to G$ と $R_a : G \to G$ を $L_a(x) = ax$, $R_a(x) = xa$ によって定める. 次の主張を確かめよ.

問 4.17^{g}　L_a と R_a は M_G の元である. また $L_e = R_e = 1_G$ が成り立つ.

問 4.18^{g}　$f : G \to M_G$, $f(a) = L_a$ とすれば, f は G から M_G への一対一の準同型写像である.

問 4.19^{*g}　a を G の元とする. a が G 内に逆元を持つための必要十分条件は, L_a と R_a とが共に全単射であることである.

§5 群の定義

定義 5.1. 半群 G 内の全ての元が逆元を持つとき G は**群** (a group) であるという. より詳しくいうと

1) G は空でない集合である.
2) G 上には演算が一つ定義されている.
3) この演算に関して G は結合法則を満たす.
4) G 内には, その全ての元 a に対して $ae = ea = a$ となる, 特別な元 e が含まれている.
5) a が G の元であれば, この a に対して $ax = xa = e$ となる G の元 x が G 内に含まれている.

の 5 条件が満たされるときに集合 G を群と呼ぶ. 交換法則を満たす群を特に**アーベル群** (an abelian group) という.

例 5.2. $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ は数の加法を演算にしてアーベル群をなす. $\boldsymbol{Z}$ は最も基本的なアーベル群である. $\boldsymbol{Q}^*$, $\boldsymbol{R}^*$, $\boldsymbol{C}^*$, によってそれぞれ, 0 でない有理数全体のなす集合, 0 でない実数全体のなす集合, 0 でない複素数全体のなす集合を表せば, $\boldsymbol{Q}^*$, $\boldsymbol{R}^*$, $\boldsymbol{C}^*$ は数の乗法を演算としてアーベル群をなす.

補題 5.3. 半群 G に対して $G_0 = \{a \in G \mid a \text{ は } G \text{ 内で逆元を持つ }\}$ と置くと, G_0 は G での積を演算に群をなす.

証明. 問題 4.12 によって G の単位元 e は G_0 に含まれる. 問 4.16 より a, b が G_0 の元であれば G での積 ab も G_0 の元である. 問 4.13 より G_0 の元の逆元は G_0 に含まれる. 以上より G_0 は G の積に関して群をなす. □

系と定義 5.4. X を空でない集合とし, $S_X = \{f \mid f \text{ は } X \text{ から } X \text{ への全単射である }\}$ と置くと, S_X は写像の合成を演算として群になる. この群 S_X を X 上の**対称群**という.

証明. $S_X = (M_X)_0$ であるので, 例題 4.6 と補題 5.3 に従う. □

定義 5.5. n を自然数とし $X = \{1, 2, 3, \cdots, n\}$ としたとき, 集合 X 上の対称群 S_X を S_n と書き, $\boldsymbol{n}$ **次の対称群** (the symmetric group of degree n) と呼ぶ.

元の個数が有限な群を有限群といい, 元の個数をその群の**位数** (order) と呼ぶ. S_n は最も基本的は有限群である. 後に示すように S_n の位数は $n!$ で, n が 3 以上ならアーベル群ではでない.

例 5.6. 座標平面の単位円上の n 個の点, $(\cos(2k\pi/n), \sin(2k\pi/n))$ $(k = 0, 1, \cdots, n-1)$ を頂点とする正 n 角形 S を考える. 原点を中心とする $2k\pi/n$ $(k = 0, 1, \cdots, n-1)$ ラジアンの回転は S を S にうつす. 直線 $\cos(k\pi/n)y = \sin(k\pi/n)x$ $(k = 0, 1, \cdots, n-1)$[15] に関する平面の折り返しも S を S にうつす. これらの $2n$ 個の操作の全体を G とする. 操作 $\sigma, \omega \in G$ に対して, 演算 $\sigma\,\omega$ を

[15]要するに直線 $y = \tan(k\pi/n)x$ なのだが, $\tan(\pi/2) = \infty$ なのでこの様に書いたのである.

二つの操作を連続して行う操作と定義する (先に ω, 後に σ を行う). このとき G は群になる (問 5.10). この群を $\boldsymbol{n}$ **次の二面体群** (the dihedral group of degree n) と呼び D_n で表す.

$f : \boldsymbol{R}^3 \to \boldsymbol{R}^3$ は原点を原点にうつし, 2 点間の距離を変えない写像とする. このとき f は線形写像である事が示される. $\|f(\boldsymbol{x})\| = \|\boldsymbol{x}\|$ が任意の $\boldsymbol{x}$ に対して成り立つので, f は直交行列 M によって $f(\boldsymbol{x}) = M\boldsymbol{x}$ と表せる. ${}^tMM = E$ より $|M| = \pm 1$ である. $|M| = -1$ の時 f は原点を含むある平面に関する対称移動が関わってくるので, $\boldsymbol{R}^3$ を一旦 4 次元空間に入れて折り返さないと実現できない. よって $|M| = 1$ の場合だけを考える. M の固有値は絶対値が 1 である. 固有値 α が虚数であれば, $\overline{\alpha}$ も固有値であり, 3 つの固有値の積が $|M|$ に等しいので, もう一つの固有値は 1 である. $\boldsymbol{p}$ を固有値 α の固有ベクトルとする時, $\overline{\boldsymbol{p}}$ は固有値 $\overline{\alpha}$ の固有ベクトルである. $\boldsymbol{q}_3$ を固有値 1 の固有ベクトルとする. $\boldsymbol{p}$, $\overline{\boldsymbol{p}}$, $\boldsymbol{q}_3$ は直交するので, 長さを 1 に取っておくと $P = (\boldsymbol{p}\ \overline{\boldsymbol{p}}\ \boldsymbol{q}_3)$ はユニタリ行列で

$$P^{-1}MP = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \overline{\alpha} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

が成り立つ. $\alpha = \cos\theta + i\sin\theta$ とおき $\boldsymbol{p} = \boldsymbol{p}_1 + i\boldsymbol{p}_2$ ($\boldsymbol{p}_1$, $\boldsymbol{p}_2$ は実ベクトル) とする. $\overline{\boldsymbol{p}} = \boldsymbol{p}_1 - i\boldsymbol{p}_2$ である. $\boldsymbol{q}_1 = \sqrt{2}\boldsymbol{p}_1$, $\boldsymbol{q}_2 = \sqrt{2}\boldsymbol{p}_2$, $\boldsymbol{q}_3$ は互いに直交して長さが 1 である事は容易に分かる. また $M\boldsymbol{p} = \alpha\boldsymbol{p}$ を実部と虚部に分けてみると

$$M\boldsymbol{q}_1 = \cos\theta\,\boldsymbol{q}_1 - \sin\theta\,\boldsymbol{q}_2, \quad M\boldsymbol{q}_2 = \sin\theta\,\boldsymbol{q}_1 + \cos\theta\,\boldsymbol{q}_2$$

が成り立つ事が分かる. 従って, $Q = (\boldsymbol{q}_1\ \boldsymbol{q}_2\ \boldsymbol{q}_3)$ は直交行列で,

$$Q^{-1}MQ = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{$*$}$$

が成り立つ. 即ち, M は $\boldsymbol{q}_3$ を含む直線を軸とする θ ラジアンの回転である.

M の固有値が全て実数の時は, $|M| = 1$ より固有値の全体は $\{1, 1, 1\}$ あるいは $\{1, -1, -1\}$ である. 前の場合 M は単位行列で, 後の場合は 直交行列 P が存在して,

$$P^{-1}MP = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

が成り立つ. よって, 前の場合は $\theta = 0$, 後の場合は $\theta = \pi$ として $(*)$ の形になっている.

例 5.7. 3 次元空間内に正四面体 V がある. V の重心を中心とする座標を入れる. 直交行列 M ($|M| = 1$) で V を V にうつすもの全体を G とする. G には下図の (a) のタイプの回転と, (b) のタイプの回転がある. (a) のタイプの回転は $2 \times 4 = 8$ 通り, (b) のタイプの回転は 3 通り, 恒等写像が 1 つあるので, G の位数は 12 である. この群を**正四面体群**という.

例 5.8. 同様に正六面体 (立方体) V を V にうつすもの全体を G とする. G には下図の (a), (b), (c), (d) のタイプの回転がある. (a), (b), (c), (d) のタイプの回転はそれぞれ, 3, $3 \times 2 = 6$, 6, $4 \times 2 = 8$ 通りあり, 恒等写像が 1 つあるので, G の位数は 24 である. この群を**正六面体群**という.

同様にして, 正八面体群, 正十二面体群, 正二十面体群が定義される.

問 5.1^h 問 4.2 の半群 G は群であることを確かめよ. G はアーベル群か.

問 5.2^h $\boldsymbol{R}^+$, $\boldsymbol{Q}^+$ は数の乗法を演算としてアーベル群をなす.

問 5.3^h $\boldsymbol{R}^n$ はベクトルの加法を演算としてアーベル群をなす.

問 5.4^h　$M_{m,n}(\boldsymbol{R})$ は行列の加法を演算としてアーベル群をなす.

問 5.5^h　$GL(n,\boldsymbol{R})$ によって n 次の実正則行列全体のなす集合を表すと, $GL(n,\boldsymbol{R})$ は行列の積を演算として群をなす. $n \geqq 2$ ならば $GL(n,\boldsymbol{R})$ はアーベル群ではない.

問 5.6^h　$SL(n,\boldsymbol{R}) = \{A \in GL(n,\boldsymbol{R}) \mid \det A = 1\}$ と置くと, $SL(n,\boldsymbol{R})$ は行列の積を演算として群をなす

問 5.7^h　$G = \{z \in \boldsymbol{C} \mid |z| = 1\}$ と置くと G は数の乗法を演算としてアーベル群をなす.

問 5.8^h　n は自然数とし, $C_n = \{z \in \boldsymbol{C} \mid z^n = 1\}$ と置くと C_n は数の乗法を演算として位数 n のアーベル群をなす.

問 5.9^h　$G_1 = \{0\}$, $G_2 = \{0,1\}$, $G_2 = \{0,1,2\}$ とし, G_1, G_1, G_2 に演算をそれぞれ次の表によって定義する. このとき G_1, G_1, G_2 はこの演算に関して群になることを確かめよ.

	0
0	0

,

	0	1
0	0	1
1	1	0

,

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

問 5.10^i　二面体群 D_n が群である事を示せ.

問 5.11^i　σ_k $(k = 0, 1, \cdots, n-1)$ を原点を中心とする $2k\pi/n$ ラジアンの回転とし, τ を x-軸に関する折り返しとする. $\tau\sigma_k$ が何かを考えて, $D_n = \{\sigma_0, \cdots, \sigma_{n-1}, \tau\sigma_0, \cdots, \tau\sigma_{n-1}\}$ である事を示せ.

問 5.12^i　直線 $\cos(m\pi/n)y = \sin(m\pi/n)x$ に関する平面の折り返しを ω とする. $\sigma_k\,\omega$ と $\omega\,\sigma_k$ を求めよ.

問 5.13^i　直線 $\cos(k\pi/n)y = \sin(k\pi/n)x$, $\cos(m\pi/n)y = \sin(m\pi/n)x$ に関する平面の折り返しをそれぞれ ω, ρ とする. $\rho\omega$ と $\omega\rho$ を求めよ.

問 5.14^i　$D_3 = \{\sigma_0, \sigma_1, \sigma_2, \tau\sigma_0, \tau\sigma_1, \tau\sigma_2\}$ の乗積表を作れ.

§6　群演算の基本的性質

G は群とする.

補題 6.1.　a, b, x, y を G の元とする.

1)　もし $ax = ay$ ならば $x = y$ である.

2)　もし $xb = yb$ ならば $x = y$ である.

3)　$a(a^{-1}x) = x$, $(xb^{-1})b = x$ である.

4)　$aa = a$ ならば $a = e$ である.

5) $ab = e$ ならば $a = b^{-1}$ かつ $b = a^{-1}$ である.

6) $(ab)^{-1} = b^{-1}a^{-1}$ である.

7) $e^{-1} = e$ である.

証明. 問 4.12 〜問 4.16 を見よ. □

系 6.2. G の任意の元 a について等式 $aa = e$ が成り立てば G はアーベル群である.

証明. 補題 6.1 の 5) より $a^{-1} = a$ が G の任意の元について成り立つ. よって a, b を G の元とすれば $(ab)^{-1} = ab$. 一方で補題 6.1 の 6) より $(ab)^{-1} = b^{-1}a^{-1} = ba$ 故に $ab = (ab)^{-1} = ba$. 従って G はアーベル群である. □

$a_1, a_2, a_3, \cdots, a_n$ を G の元とする. このとき

$$\begin{aligned} a_1a_2a_3 &= (a_1a_2)a_3 \\ a_1a_2a_3a_4 &= ((a_1a_2)a_3)a_4 \\ &\vdots \\ a_1a_2a_3\cdots a_n &= ((\cdots((a_1a_2)a_3)\cdots)a_{n-1})a_n \end{aligned}$$

によって積 $a_1a_2a_3\cdots a_n$ を定義する. よって n が 2 以上であれば

$$a_1a_2a_3\cdots a_n = (a_1a_2a_3\cdots a_{n-1})a_n$$

である.

G がアーベル群のときは, 数の足し算をモデルにして, 群の演算も加法 $+$ で表示し $a+b$ を a, b の**和**ということが多い. この場合, 記号 0 (ゼロ) を用いて単位元を表し, $-a$ を用いて元 a の逆元を表す. すると G の元 $a_1, a_2, a_3, \cdots, a_n$ に対して

$$\begin{aligned} a_1 + a_2 + a_3 &= (a_1 + a_2) + a_3 \\ a_1 + a_2 + a_3 + a_4 &= ((a_1 + a_2) + a_3) + a_4 \\ &\vdots \\ a_1 + a_2 + a_3 + \cdots + a_n &= ((\cdots((a_1 + a_2) + a_3)\cdots) + a_{n-1}) + a_n \end{aligned}$$

によって和 $a_1 + a_2 + a_3 + \cdots + a_n$ を定義する. n が 2 以上であれば

$$a_1 + a_2 + a_3 + \cdots + a_n = (a_1 + a_2 + a_3 + \cdots + a_{n-1}) + a_n$$

である.

次の命題 6.3 の 1) は群内での積は, 順序を入れ換えない限り, どのように括弧で括っても同じ値をとることを示している.

命題 6.3.

1) $(a_1a_2\cdots a_n)(b_1b_2\cdots b_m) = a_1a_2\cdots a_nb_1b_2\cdots b_m$.

2) G がアーベル群で演算が加法 $+$ で表示されているときは,

$$(a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_m) = a_1 + a_2 + \cdots + a_n + b_1 + b_2 + \cdots + b_m$$

が成り立つ.

証明. 1) のみ証明する. 2) は 1) から従う. m についての数学的帰納法で証明する. $m = 1$ のときは定義による. $m \geqq 2$ であって $m-1$ までは主張は正しいと仮定する. このとき $b_1b_2\cdots b_m = (b_1b_2\cdots b_{m-1})b_m$ であるから,

$$\begin{aligned}(a_1a_2\cdots a_n)(b_1b_2\cdots b_m) &= (a_1a_2\cdots a_n)((b_1b_2\cdots b_{m-1})b_m) \\ &= ((a_1a_2\cdots a_n)(b_1b_2\cdots b_{m-1}))b_m \qquad \text{(結合法則による)} \\ &= (a_1a_2\cdots a_nb_1b_2\cdots b_{m-1})b_m \qquad \text{(帰納法の仮定による)} \\ &= a_1a_2\cdots a_nb_1b_2\cdots b_{m-1}b_m \qquad \text{(定義による).}\end{aligned}$$

□

特に $a_1 = a_2 = \cdots = a_n = a$ のときは, $a_1a_2\cdots a_n = a^n$ と書き **a の n 乗** と読む. ここで n は勿論自然数であるが, n が負の整数のときは $a^n = (a^{-1})^{-n}$ と定める. また $a^0 = e$ と置く. この定義によれば G の任意の元 a について $a^1 = a$ であって, a の -1 乗は a の逆元 a^{-1} に他ならない. また $e^n = e$ が全ての整数 n について成り立つ.

G がアーベル群で演算が加法 $+$ で表示されている場合には, $a_1 = a_2 = \cdots = a_n = a$ に対して $a_1 + a_2 + \cdots + a_n = na$ と書き **a の n 倍** と読む. n が負の整数のときは $na = (-n)(-a)$ と定める. この定義によれば G の任意の元 a について $1a = a$ であって, a の -1 倍は a の逆元 $-a$ に他ならない. また $n0 = 0$ が全ての整数 n について成り立つ.

指数法則 (問 6.2 及び問 6.3) は極めて重要である.

例題 6.4. 群 G が 4 個の元よりなれば G はアーベル群である.

証明. $G = \{e, a, b, c\}$ とする. 但し e は G の単位元である. さて G の 5 個の元の列 $e = a^0$, $a = a^1$, a^2, a^3, a^4 の中には同じものが存在するので, $a^i = a^j$ がある $0 \leqq i < j \leqq 4$ について成り立つ. 問 6.2 より $a^{j-i} = e$ である. よって $a \neq e$ であるから, a^2, a^3, a^4 のいずれかは e と等しいことが分かる. $a^n = e$ となる自然数 n を最小にとろう (勿論 $n = 2, 3$ 又は 4 である). すると G の n 個の元 $e = a^0$, $a = a^1$, $\cdots$, a^{n-1} はどの二つも等しくない. 実際もし $a^i = a^j$ がある $0 \leqq i < j \leqq n-1$ について成り立つならば問 6.2 より $a^{j-i} = e$ であるが, $j - i$ は自然数で n よりも本当に小さいから, n の最小性に反する. よって $e = a^0$, $a = a^1$, $\cdots$, a^{n-1} はどの二つも等しくない. そこでもし $n = 4$ であれば $G = \{e, a, a^2, a^3\}$ であって, 指数法則 (問 6.2) より確かに G はアーベル群である[16].

[16] この群を位数 4 の巡回群という.

よって以後 $n \leqq 3$ であるとする. この議論は b, c についても有効であるから, $b^m = e$, $c^k = e$ となる最小の自然数 m, k はそれぞれ 3 以下であるとしてよい. すると $n = 2$ である. 実際可能性はあと $n = 3$ しかないのであるが, このときは $e = a^0$, $a = a^1$, a^2 が相異なるため $b = a^2$ か又は $c = a^2$ が成り立つ. 一般性を失うことなく $b = a^2$ としてよい. すると $G = \{e, a, a^2, c\}$ を得る. また $a^3 = e$ ($n = 3$ であるので) より $b = a^2 = a^{-1}$ である. このとき補題 6.1 を用いれば ac は e, a, a^2, c のどれとも等しくないことが容易に確かめられる. よって $n = 2$ であって $a^2 = e$ となる. この議論は b, c についても有効であるから $a^2 = b^2 = c^2 = e$ となり系 6.2 より G はアーベル群である[17]. □

定理 6.5. $f : G \to S_G$, $f(a) = L_a$ は準同型写像で単射である.

証明. まず f が準同型写像であることと単射であることは既に問 4.18 で証明済みである. (半群に対して成り立つことは当然群に対しても成り立つ.) 問題は L_a が S_G に属することである. L_a が単射であることは補題 6.1 の 1) による. 任意の $y \in G$ に対して $x = a^{-1}y$ と置くと, $L_a(x) = a(a^{-1}y) = (aa^{-1})y = ey = y$ となるので L_a は全射でもある. □

問 6.1 等式 $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ を証明せよ.

問 6.2^j a, b は G の元で m, n は整数とする. 等式 $a^m a^n = a^{m+n}$ と $(a^m)^n = a^{mn}$ とを証明せよ.

問 6.3^j G がアーベル群で演算が加法 $+$ で表示されているときは, $(m+n)a = ma + na$, $n(a+b) = na + nb$[18], $m(na) = (mn)a$ が成り立つことを証明せよ.

問 6.4 位数が高々 5 の群はアーベル群であることを確かめよ[19].

問 6.5 群 G 上に関係 $\sim$[20] を

$$\sim = \{(a, b) \mid a, b \in G \text{ であって } a = tbt^{-1} \text{ となる元 } t \text{ が } G \text{ 内に存在する } \}$$

によって定めると, $\sim$ は集合 G 上の同値関係であることを確かめよ.

問 6.6 $G = S_3$ の元を問 6.5 の同値関係によって類に分けよ.

問 6.7 G は群とする. 次の主張を確かめよ.

1) G の元 a に対して写像 $i_a : G \to G$ を $i_a(x) = axa^{-1}$ によって定義すると, i_a は同型写像であり従って S_G の元である.

2) 写像 $f : G \to S_G$ を $f(a) = i_a$ とすれば f は準同型写像である.

---

[17] この群を Klein の 4 元群という.
[18] もっと一般的に G がアーベル群でない場合でも, $ab = ba$ ならば $(ab)^n = a^n b^n$ が成り立つことを示せ.
[19] 従って有限群でアーベル群でないものの位数は 6 から始まり S_3 がその最初の例である.
[20] チルダと読む.

§7 対称群 S_n

自然数 n に対して集合 $X=\{1,2,3,\cdots,n\}$ 上の対称群 S_X を S_n と書き n 次の対称群という. 従って $S_n=\{s \mid s$ は X から X への全単射である $\}$ であって, 写像の合成を演算とし単位元 e は X 上の恒等写像 1_X である. また S_n の元 s の逆元は s の逆写像に等しい (cf.[21] 系 4.7, 系と定義 5.4).

s を S_n の元とすれば, s は単射であるから $s(1)$, $s(2)$, $\cdots$, $s(n)$ はどの二つも互いに異なっていてかつ集合 X に属するので, $s(1)$, $s(2)$, $\cdots$, $s(n)$ は 1, 2, $\cdots$, n の順列である. 逆に i_1, i_2, $\cdots$, i_n を 1, 2, $\cdots$, n の順列とし, X から X への写像 $s:X\to X$ を $s(1)=i_1$, $s(2)=i_2$, $\cdots$, $s(n)=i_n$ によって定義すると, s は単射であるのみでなく, 文字 1, 2, $\cdots$, n は必ず i_1, i_2, $\cdots$, i_n 内のどこかに出現するのであるから s は全射でもあり, s は全単射即ち S_n の元である. つまり S_n の元を一つ与えることと 1, 2, $\cdots$, n の順列を一つ与えることは同値である. この故 S_n の元を n 文字の**置換**と呼ぶ. 特にこれより S_n の位数は $n!$ であることが分かる.

1, 2, $\cdots$, n の順列 i_1, i_2, $\cdots$, i_n に対して $s(1)=i_1$, $s(2)=i_2$, $\cdots$, $s(n)=i_n$ によって定まる S_n の元を

$$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$$

で表す[22]. この記法によれば

$$\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}=e \text{ であって, } \begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix} \text{ となる.}$$

簡単のため $n=3$ としてみよう. 1, 2, 3 の順列は全部で 6 個あり S_3 の元を書き出すと,

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$

である. $e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ であり, $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}=\begin{pmatrix}1&3&2\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ となる. また $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ である[23]. 簡単のためその置換によって動いていない文字を省くことにしたい. 例えば

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}2&3\\3&2\end{pmatrix}, \text{ 更にこれを単に } (23) \text{ と書く.}$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2\\2&1\end{pmatrix}, \text{ 更にこれを単に } (12) \text{ と書く.}$$
$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&3\\3&1\end{pmatrix}, \text{ 更にこれを単に } (13) \text{ と書く.}$$

---

[21] cf. は「$\cdots$ を参照せよ」の意味である.
[22] これは一般的な書き方である.
[23] ここでは置換は写像の一種と考えているので, 二つの置換の積は右の置換を先に行って左の置換を後に行ったものと定義している. 但し, 本によっては積の定義が逆になっているものもあるので, 他の本を読む場合には注意が必要である.

そして $a=(23)$, $b=(12)$, $c=(13)$, $f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ と置き S_3 の積の表 (乗積表という) を作ってみると下のようになる.

	e	a	b	c	f	g
e	e	a	b	c	f	g
a	a	e				
b	b		e			
c	c			e		
f	f					e
g	g				e	

文字 $a_1, a_2, \cdots, a_m$ に対して, a_1 を a_2 に, a_2 を a_3 に, $\cdots$, a_{m-1} を a_m に, そして a_m を a_1 に移す置換を長さ m の巡回置換といって $(a_1a_2\cdots a_m)$ と書く.

$$(a_1a_2\cdots a_m)=(a_ma_1)(a_{m-1}a_1)\cdots(a_2a_1)$$

が成り立つ (問 7.3). 長さ 2 の巡回置換を互換という. 長さ 1 の巡回置換は e に等しい.

補題 7.1. 全ての置換は共通文字のない巡回置換の積として表すことができる.

証明. S_n の元 s に対して集合 $I(s)=\{i\in X \mid s(i)\neq i\}$ を考える. 即ち $I(s)$ は置換 s によって動いてしまう文字の全体よりなる集合である. さて共通文字のない巡回置換の積として表すことができないような, 元 s が S_n 内に存在したと仮定し, そのような悪い s の中から集合 $I(s)$ の元の個数 $|I(s)|$ が最も小さいもの (の一つ) を取る. すると少なくとも $I(s)$ は空集合ではないから, $s(i)\neq i$ であるような文字 i を X 内に取れる. ここで無限の文字列 $s^0(i)=i$, $s(i)$, $s^2(i)$, $s^3(i)$, $\cdots$, $s^m(i)$, $\cdots$, には同じ文字が存在するので, $s^k(i)=s^m(i)$ が成り立つ自然数 k, m で $0\leqq k<m$ なるものが存在する. このとき $s^{m-k}(i)=i$ である. $s^n(i)=i$ である最小の自然数を n とすれば, $n\geqq 2$ であって n の最小性より, $s^0(i)=i$, $s(i)$, $s^2(i)$, $\cdots$, $s^n(i)$ は全て相異なるはずである. そこで巡回置換 $(i, s(i), s^2(i), \cdots, s^{n-1}(i))$ を考え, これを t と置き $u=st^{-1}$ を調べることにする. まず $I(u)$ は $I(s)$ の部分集合である. 更に $s^0(i)=i$, $s(i)$, $s^2(i)$, $\cdots$, $s^{n-1}(i)$ は全て $I(s)$ の元であって, しかもどれも $I(u)$ の元でなあり得ない. よって少なくとも $|I(u)|<|I(s)|$ であり従って n の最小性より, u は共通文字のない巡回置換の積として表すことができるはずである. 今 $u=s_0s_1\cdots s_r$ がそのような積であるとせよ. すると $s=s_0s_1\cdots s_rt$ である. しかも $s^0(i)=i$, $s(i)$, $s^2(i)$, $\cdots$, $s^{n-1}(i)$ はどれも $I(u)$ の元ではないので, s_1 から s_r までに現れる文字はどれも t では動かない. つまり s_1 から s_r までと t には共通文字がない. これは s が共通文字のない巡回置換の積として表すことができないという仮定に反する. □

補題 7.1 と問 7.3 より直ちに次を得る.

定理 7.2. n が 2 以上であれば S_n の元は全て互換の積である.

この定理は何個かのものを並べ換えるには, 二つずつの並べ換えを何回か繰り返して行えばよいという, 経験則の数学的証明である.

例題 7.3. 次の置換 s を互換の積として表すと

$$\begin{aligned} s &= \begin{pmatrix} 1 & 15 & 7 & 6 & 11 & 3 & 2 & 14 & 4 & 10 & 13 & 5 & 9 & 12 & 8 \\ 3 & 8 & 13 & 15 & 4 & 14 & 9 & 1 & 6 & 2 & 12 & 10 & 5 & 7 & 11 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 14 \\ 3 & 14 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 & 9 & 5 & 10 \\ 9 & 5 & 10 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 6 & 15 & 8 & 11 \\ 6 & 15 & 8 & 11 & 4 \end{pmatrix} \circ \begin{pmatrix} 7 & 13 & 12 \\ 13 & 12 & 7 \end{pmatrix} \\ &= (1,3,14)(2,9,5,10)(4,6,15,8,11)(7,13,12) \\ &= (14,1)(13,1)(10,2)(5,2)(9,2)(11,4)(8,4)(15,4)(6,4)(12,7)(13,7) \end{aligned}$$

である.

定義 7.4. S_n の元 s に対して $\mathrm{sgn}(s) = \prod_{i<j}(s(j)-s(i))/(j-i)$ と置き s の符号という. なお $n=1$ のときは $\mathrm{sgn}(s)=1$ と考える.

次の結果が基本的である.

補題 7.5.

1) $\mathrm{sgn}(s) = 1$ 又は $\mathrm{sgn}(s) = -1$ である.

2) s が互換であれば $\mathrm{sgn}(s) = -1$ である.

3) s, t が S_n の元であれば, $\mathrm{sgn}(st) = \mathrm{sgn}(s)\mathrm{sgn}(t)$ である.

証明 1)
$$\begin{aligned} (\mathrm{sgn}(s))^2 &= \Big(\textstyle\prod_{i<j}(s(i)-s(j))/(i-j)\Big) \cdot \Big(\prod_{i<j}(s(j)-s(i))/(j-i)\Big) \\ &= \Big(\textstyle\prod_{i<j}(s(i)-s(j)) \cdot \prod_{i<j}(s(j)-s(i))\Big) \,/\, \Big(\prod_{i<j}(i-j) \cdot \prod_{i<j}(j-i)\Big) \\ &= \Big(\textstyle\prod_{i<j}(s(i)-s(j)) \cdot \prod_{j<i}(s(i)-s(j))\Big) \,/\, \Big(\prod_{i<j}(i-j) \cdot \prod_{j<i}(i-j)\Big) \\ &= \textstyle\prod_{i\neq j}(s(i)-s(j)) / \prod_{i\neq j}(i-j) \\ &= \textstyle\prod_{i\neq j}(i-j) / \prod_{i\neq j}(i-j) \\ &= 1 \end{aligned}$$

である. 故に $\mathrm{sgn}(s) = \pm 1$ である.

2) $s = (a,b)$ $(a<b)$ とする. このとき $\mathrm{sgn}(s) = \prod_{i<j}(s(j)-s(i))/(j-i)$ は, $i<j$ であってしかし $s(i) > s(j)$ となる組 (i,j) の個数 (逆転数) で決まる.

$$s = (a,b) = \begin{pmatrix} 1 & \cdots & a-1 & a & a+1 & \cdots & b-1 & b & b+1 & \cdots & n \\ 1 & \cdots & a-1 & b & a+1 & \cdots & b-1 & a & b+1 & \cdots & n \end{pmatrix}$$

であるから, s の逆転数は, $i=a$ のときに $b-a$ 回, $i = a+1, a+2, \cdots, b-1$ がそれぞれ 1 回ずつで計 $b-1-a$ 回, 合計 $(b-a)+(b-1-a)$ 回で奇数である.

3) $\mathrm{sgn}(st) = \prod_{i<j}((st)(j) - (st)(i))/(j-i)$
$= \prod_{i<j}(s(t(j)) - s(t(i)))/(j-i)$
$= \left(\prod_{i<j}(s(t(j)) - s(t(i)))/(t(j)-t(i))\right) \cdot \left(\prod_{i<j}(t(j)-t(i))/(j-i)\right)$
$= \mathrm{sgn}(s)\mathrm{sgn}(t).$ □

定理 7.6. n は 2 以上とする. S_n の元 s を互換の積 $s = s_1 s_2 \cdots s_r$ として表したとき, r が偶数であるか奇数であるかは, 表現 $s = s_1 s_2 \cdots s_r$ のとりかたにはよらず s のみで定まる.

証明. 補題 7.5 の 3) より $s = s_1 s_2 \cdots s_r$ なら $\mathrm{sgn}(s) = (-1)^r$ であることに従う. □

定義 7.7. $\mathrm{sgn}(s) = 1$ である置換 $s \in S_n$ を**偶置換**, $\mathrm{sgn}(s) = -1$ である置換 $s \in S_n$ を**奇置換**という. 互換は全て奇置換である. e は偶置換であって, 偶置換と偶置換の積は偶置換となる. 偶置換の全体よりなる S_n の部分集合を A_n と書く. 即ち $A_n = \{s \in S_n \mid \mathrm{sgn}(s) = 1\}$ である.

命題 7.8. $s, t \in S_n$ が同じ文字を含まないならば, $st = ts$ である.

証明. $1 \leqq i \leqq n$ とする. 仮定により i は s と t の片方のみに含まれるか, あるいは双方に含まれない. 後の場合は $s(i) = t(i) = i$ であるから, $st(i) = ts(i) = i$ である. 前の場合, i は s のみに含まれるとする. $s(i) = j$ とする. j は s に含まれるので, 仮定により t には含まれない. 従って $t(i) = i$, $t(j) = j$ である. よって $st(i) = s(i) = j$, $ts(i) = t(j) = j$ で $st(i) = ts(i)$ である. 全ての i について上のことが成り立つので $st = ts$. □

問 7.1 S_3 の乗積表を完成せよ. そして $n \geqq 3$ なら S_n はアーベル群でないことを確かめよ.

問 7.2 S_4 の元を全て書き出しその乗積表を作れ.

問 7.3 $(a_1 a_2 \cdots a_m) = (a_m a_1)(a_{m-1} a_1) \cdots (a_2 a_1)$ が成り立つことを (帰納法で) 確かめよ.

問 7.4 〜問 7.8 次の置換を互換の積として表せ.

問 7.4^k $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 8 & 13 & 15 & 4 & 14 & 9 & 1 & 6 & 2 & 12 & 10 & 5 & 7 & 11 \end{pmatrix}$.

問 7.5^k $\begin{pmatrix} 1 & 15 & 7 & 6 & 11 & 3 & 2 & 14 & 4 & 10 & 13 & 5 & 9 & 12 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \end{pmatrix}$.

問 7.6^k $\begin{pmatrix} 2 & 15 & 8 & 6 & 10 & 3 & 1 & 14 & 5 & 11 & 13 & 4 & 9 & 12 & 7 \\ 3 & 8 & 13 & 15 & 4 & 14 & 9 & 1 & 6 & 2 & 12 & 10 & 5 & 7 & 11 \end{pmatrix}$.

問 7.7^k $\begin{pmatrix} 1 & 15 & 7 & 6 & 11 & 3 & 2 & 14 & 4 & 8 & 13 & 5 & 9 & 12 & 10 \\ 8 & 3 & 13 & 15 & 2 & 14 & 9 & 1 & 6 & 4 & 12 & 10 & 5 & 11 & 7 \end{pmatrix}$.

問 7.8^k $\begin{pmatrix} 1 & 15 & 7 & 2 & 11 & 3 & 10 & 14 & 4 & 6 & 13 & 5 & 12 & 9 & 8 \\ 3 & 11 & 13 & 15 & 4 & 14 & 5 & 1 & 7 & 2 & 12 & 10 & 9 & 6 & 8 \end{pmatrix}$.

問 7.9 A_4 の元を全て書き出し, これらを互換の積として表せ.

§8 部分群 (subgroups)

G は群とする.

定義と定理 8.1. 集合 H が G の部分群であるとは, H が次の 2 条件を満たすことをいう.

1) H は G の空でない部分集合である.

2) a, b が H の元であれば, ab^{-1} も H の元である.

このとき $e \in H$ であって H の任意の元 a, b について ab, a^{-1} は H に属する. 従って H は G での積を演算にして独立した群となる.

証明. H は G の部分群とせよ. すると条件 1) によって H は少なくとも一つはの元を含む. これを c とすると, 条件 2) より $e = cc^{-1}$ は H に含まれる. a, b を H の元とすれば, 条件 2) より $b^{-1} = eb^{-1}$ は H の元であり, 従って $ab = a(b^{-1})^{-1}$ も H の元となる. 故に G での積は集合 H 上に演算を引き起こし, この演算について H は群をなす. □

例えば $\{e\}$ と G は G の部分群である. G の部分群は必ず集合 $\{e\}$ を含む. G の元 a に対して $H = \{a^n \mid n \in \boldsymbol{Z}\}$ と置けば H は G の部分群である. この部分群 H は元 a のみで定まるから, これを元 a で生成された G の部分群と呼び $\langle a \rangle$ と書く. また加法群 $\boldsymbol{Z}$ は加法群 $\boldsymbol{R}$ の部分群である. $SL(n, \boldsymbol{R})$ は $GL(n, \boldsymbol{R})$ の部分群である. A_n は S_n の部分群をなし n 次の**交代群**[24] と呼ばれる. この他にも数学の各分野で非常に多くの部分群の例が見いだされるであろう. 群構造の研究とはいかなる部分群をどの位多様に含むかの解析であるといってもさほど言い過ぎではないのである.

補題 8.2. G の空でない有限部分集合 H が G の積について閉じている, 即ち, 条件

$$\underline{a, b \text{ が } H \text{ の元であれば } ab \text{ も } H \text{ の元である}}$$

を満たすならば, H は G の部分群である.

証明. a, b を H の元とせよ. すると条件より b のベキ $b = b^1, b^2, b^3, \cdots, b^n, \cdots$ は全て H の元である. H は有限であるから, これらの中には同じものが存在し, 指数法則によって $b^n = e$ となる自然数 n が必ず存在する. $n \geqq 2$ であれば $b^{-1} = b^{n-1}$ であるから, b^{-1} は H の元である. $n = 1$ であれば $b = e$ であるから, やはり $b^{-1} = e = b$ は H の元である. a, b が H の元であれば, 仮定より ab^{-1} も H の元であって, H は G の部分群となる. □

例 8.3. S_3 の 6 つの部分集合, $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, $\{e, f, g\}$, S_3 自身, は S_3 の積に関して閉じているので S_3 の部分群をなす.

例 8.4. 次の 6 つの正則行列をそれぞれ e, a, b, c, f, g とする. $G = \{e, a, b, c, f, g\}$ とすれば, G は $GL(3, \boldsymbol{R})$ の部分集合であってかつ行列の積について閉じている. 従って G は $GL(3, \boldsymbol{R})$ の部分

[24] $s \in S_n$ とし $f(x_1, x_2, \cdots, x_n)$ を n 変数の多項式とする. $(sf)(x_1, x_2, \cdots, x_n) = f(x_{s(1)}, x_{s(2)}, \cdots, x_{s(n)})$ と置く. f が対称式であれば $sf = f$ が成り立つ. 即ち S_n の元は対称式を不変にする. $s \in A_n$ であれば s は交代式も不変にする. 以上が対称群・交代群の名前の由来である.

群である.

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}.$$

H が G の部分群であれば, H を用いて集合 G 上に同値関係を二通り定義することができる. 一つは $\mathrm{R}_1=\{(a,b)\in G\times G\mid a^{-1}b\in H\}$ で, もう一つは $\mathrm{R}_2=\{(a,b)\in G\times G\mid ab^{-1}\in H\}$ である. ここで R_1 が同値関係であることを確かめておく. まず a が H の元であれば, $a^{-1}a=e$ で定義と定理 8.1 より e は H の元であるから, (a,a) は R_1 に含まれる. 即ち $a\mathrm{R}_1a$ である. もし $a\mathrm{R}_1b$ であれば $a^{-1}b$ は H の元であるが, H は G の部分群であるから定義と定理 8.1 より $b^{-1}a=(a^{-1}b)^{-1}$ も H に含まれ $b\mathrm{R}_1a$ を得る. $a\mathrm{R}_1b$ かつ $b\mathrm{R}_1a$ であれば, $a^{-1}b$ と $b^{-1}c$ は H の元で, 従って積 $a^{-1}c=(a^{-1}b)(b^{-1}c)$ も定義と定理 8.1 より H の元である. 故に $a\mathrm{R}_1c$. 同様にして R_2 も集合 G 上の同値関係であることが確かめられる. この議論で H が G の部分群であるという仮定が, 過不足なく使われていることに十分注目して欲しい.

a を G の元とすると, 関係 R_1 による a を含む同値類は集合 $aH=\{ah\mid h\in H\}$ に一致し, 関係 R_2 による a を含む同値類は集合 $Ha=\{ha\mid h\in H\}$ に等しい. 実際, 関係 R_1 による a を含む同値類を $C(a)$ とし x を $C(a)$ の任意の元とすれば, $x\mathrm{R}_1a$ より $a^{-1}x$ は H の元である. よって $x=ah$ $(h\in H)$ となり, x は aH に含まれることが分かる. 逆に x を集合 aH の任意の元とし, $x=ah$ $(h\in H)$ となるような H の元 h をとると $a^{-1}x=h$ であるから, $a\mathrm{R}_1x$ を得る. よって x は $\mathrm{C}(a)$ の元. 従って $\mathrm{C}(a)=aH$. 同様にして関係 R_2 による a を含む同値類は集合 Ha に等しいことが示される (必ずこれを確かめよ). 一方で写像 $f_1:H\to aH$ と写像 $f_2:H\to Ha$ とをそれぞれ $f_1(h)=ah$ と $f_2(h)=ha$ によって定義すると, 補題 6.1 の 1) と 2) によって, f_1 と f_2 はどちらも単射であり明らかに全射でもある. 従って H と aH 及び Ha とはその元の個数が全て等しい.

有限集合 X に対してその元の個数を $|X|$ で表す. 次の定理は極めて重要である.

Lagrange の定理 8.5. G は有限群とし H をその部分群とする. このとき商集合 G/R_1 と G/R_2 とは同じ個数の元よりなり, その個数は $|G|/|H|$ に等しい.

証明. $a_1,\ a_2,\ \cdots,\ a_n$ 商集合 G/R_1 の完全代表系とする. 集合族 $\{a_1H,a_2H,\cdots,a_nH\}$ は G を分割している. 各同値類は全て $|H|$ 個の元よりなり, しかも同値類は $|G/\mathrm{R}_1|$ 個あるから, $|G|=|G/\mathrm{R}_1|\cdot|H|$ である. 同様に $|G|=|G/\mathrm{R}_2|\cdot|H|$ であるので, $|G/\mathrm{R}_1|=|G|/|H|=|G/\mathrm{R}_2|$ を得る. □

例題と定義 8.6. G/R_1 から G/R_2 への全単射 $h:G/\mathrm{R}_1\to G/\mathrm{R}_2$ で, 全ての $a\in G$ について $h(aH)=Ha^{-1}$ を満たすものが存在する. 従って商集合 G/R_1 と G/R_2 とは同じ個数の元よりなる. この共通の個数を G の H に関する指数 (the index of G with respect to H) といい $[G:H]$ で表す.

証明. $f : G \to G/\mathrm{R}_1$ を自然な写像 (即ち, $f(a) = aH$, $a \in G$) とし, 写像 $g : G \to G/\mathrm{R}_2$ を $g(a) = Ha^{-1}$ によって定める. $g(a^{-1}) = H(a^{-1})^{-1} = Ha$ であるから g は全射である. 写像 g の定める G 上の同値関係 R_g を調べる. 定義により $\mathrm{R}_g = \{(a, b) \in G \times G \mid g(a) = g(b)\}$ である. a, b を G の元とすれば, $g(a) = g(b)$ であることは, g の定義より, $Ha^{-1} = Hb^{-1}$ であることと同値である. 後者は定理 1.2 より $a^{-1}\mathrm{R}_2 b^{-1}$ と同値であって, R_2 の定義よりこれは $a^{-1}(b^{-1})^{-1} \in H$, 即ち $a^{-1}b \in H$ と同値である. $a^{-1}b$ が H の元であることは定義より $(a, b) \in \mathrm{R}_1$ であるということであるから, つまり $\mathrm{R}_g = \mathrm{R}_1$ を得る. よって主張は系 2.6 に従う. □

Cauchy の定理 8.7. G は有限群とし H をその部分群とすれば $|H| \mid |G|$ である.

証明. 定理 8.5 より直ちに従う. □

例題 8.8. S_3 の部分群は $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, $A_3 = \{e, f, g\}$, S_3 自身, の合計 6 個のみである.

証明. H を $G = S_3$ の部分群とすると, 定理 8.7 より $|H|$ は 6 の約数であるから, $|H| = 1$, 2, 3 又は 6 である. $|H| = 1$ なら $H = \{e\}$ であるし, $|H| = 6$ ならば $H = G$ である. $|H| = 2$ であれば, $H = \{e, x\}$ と書くと, $x^2 \neq x$ であるから ($x^2 = x$ なら $x = e$ となる) 必ず $x^2 = e$ である. $G = S_3$ 内で $x \neq e$ であって $x^2 = e$ を満たす元は, $x = a$, b, c であるから $H = \{e, a\}$, $\{e, b\}$ 又は $\{e, c\}$ である. 次に $|H| = 3$ であると仮定しよう. $H = \{e, x, y\}$ とする. 補題 6.1 の 1) と 2) より $xy \neq x$, $xy \neq y$ であるから, $xy = e$ である. $x^2 \neq x$ であるから, $x^2 = e$ 又は $x^2 = y$ であるが, $x^2 = e$ とすると $y = ey = (x^2)y = x(xy) = xe = x$ となって矛盾. よって $x = f$ 又は $x = g$ である. y についても同様であるから, $H = \{e, f, g\}$ を得る. 以上より S_3 の部分群は $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, $\{e, f, g\}$, S_3 の合計 6 個であることが分かる. この内 $A_3 = \{e, f, g\}$ である. □

例題 8.9. n が 2 以上なら交代群 A_n は $n!/2$ 個の元よりなる. よって $[S_n : A_n] = 2$ である.

証明. B_n によって n 次の奇置換全体よりなる集合を表す. $t = (1, 2)$ と置き, 写像 $f : A_n \to B_n$ を $f(s) = st$ で定めると, f は全単射であることが容易に確かめられる. 従って $|A_n| = |B_n|$ である. $|A_n| + |B_n| = n!$ であるから, $|A_n| = n!/2$ が得られる. □

例題 8.10. 群 G の元の個数が素数ならば, G は $\{e\}$ と G 自身しか部分群を持たない. 従って問 8.7 の群 C_n は n が素数のときには, $\{e\}$ と C_n 自身しか部分群を含まない.

証明. H を G の部分群とすると, $|H|$ は $p = |G|$ の約数である. p は素数であるので $|H| = 1$ か又は $|H| = p$. 即ち, $H = \{e\}$ であるか又は $H = G$ である. □

例 8.11. n 次の直交行列の全体は群をなす. それを n 次の直交群と呼び $O(n, \boldsymbol{R})$ で表す. 即ち $O(n, \boldsymbol{R}) = \{M \in M_n(\boldsymbol{R}) \mid {}^tMM = E\}$ である. n 次の直交行列で行列式が 1 であるものの全体は群をなす. それを n 次の特殊直交群と呼び $SO(n, \boldsymbol{R})$ で表す. 即ち $SO(n, \boldsymbol{R}) = \{M \in M_n(\boldsymbol{R}) \mid {}^tMM = E,\ |M| = 1\}$ である. 二面体群 D_n は $O(2, \boldsymbol{R})$ の部分群であり, 正四面体群, 正六面体群

は $SO(3,\boldsymbol{R})$ の部分群である．正四面体群の元は四つの面の置換を引き起こすので, S_4 の部分群とも考えられる．正四面体群の位数は 12 であった．これは S_4 の位数 24 の約数である．正六面体群の元は六つの面の置換を引き起こすので, S_6 の部分群とも考えられる．正六面体群の位数は 24 であった．これは S_6 の位数 720 の約数である．

問 8.1　H が G の部分群で, K が H の部分群であれば, K は G の部分群であることを確かめよ．

問 8.2　$\{H_\alpha\}_{\alpha\in A}$[25] が G の部分群の族であれば, H_α 全ての共通部分は必ず G の部分群であることを示せ．

問 8.3　部分群の和集合は必ずしも部分群ではない．例を挙げよ．

問 8.4　乗積表を作って例 8.4 を確かめよ．またこの群の乗積表を S_3 の乗積表と比較せよ．

問 8.5　e, a, b, c をそれぞれ次の 4 つの行列とする．

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix},\begin{pmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{pmatrix},\begin{pmatrix}0&0&0&-1\\0&0&-1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

このとき次の主張を証明せよ．

1)　$a^2=b^2=c^2=-e$, $ab=-ba=c$, $bc=-cb=a$, $ca=-ac=b$ である．

2)　$G=\{e,a,a^2,a^3,b,ab,a^2b,a^3b\}$ は $GL(4,\boldsymbol{R})$ の部分群である．(乗積表を作れ.)

3)　G は位数 2 の部分群を唯一つしか含まない．

問 8.6　$H=\{e,(12),(34),(12)(34)\}$ は S_4 の部分群であることを確かめよ．

問 8.7　n を自然数とし $C_n=\{z\in\boldsymbol{C}\mid z^n=1\}$ と置く．C_n は $\boldsymbol{C}^*=\{z\in\boldsymbol{C}\mid z\neq 0\}$ の部分群であることを確かめよ．

問 8.8　C_4 の乗積表を作り問 8.6 の H の乗積表と比較せよ．

問 8.9　R_2 は G 上の同値関係であることを確かめよ．

問 8.10　$\mathrm{R}_1=\mathrm{R}_2$ であるための必要かつ十分な条件は, G の全ての元 a について $aH=Ha$ が成り立つことであることを証明せよ．

問 8.11　G の全ての元 a について $aH=Ha$ が成り立つための必要かつ十分な条件は, G の全ての元 a と H の全ての元 h について $aha^{-1}\in H$ であることを証明せよ．

問 8.12　A_4 の部分群を全て求めよ．

---

[25] A は添え字 α の集合である．A が有限集合のときは $A=\{1,2,\cdots,n\}$ として $\{H_\alpha\}_{\alpha\in A}=\{H_1,H_2,\cdots,H_n\}$ と表せる．また A が可算無限集合のときは $\{H_\alpha\}_{\alpha\in A}=\{H_1,H_2,\cdots,H_n,\cdots\}$ と表せる．しかし A が可算でない無限集合のときはこのような表し方はできない．例えば k を実数として $H_k=\{(x,kx)\mid x\in\boldsymbol{R}\}$ とすると H_k は $\boldsymbol{R}^2$ の部分群である．この H_k の集合族は $\{H_k\}_{k\in\boldsymbol{R}}$ と表すより他にない．

§9 群の作用 (group actions)

定義 9.1. G は群で X は空でない集合とする. G が X に作用するとは, G の X への作用 (an action of G on X), 即ち, 直積集合 $G \times X$ から集合 X への写像 $m : G \times X \to X$ で, 次の条件を満たすものが一つ与えられていることをいう.

1) 全ての $a, b \in G$ と全ての $x \in X$ に対して, $m(a, m(b, x)) = m(ab, x)$ が成り立つ.

2) 全ての $x \in X$ に対して, $m(e, x) = x$ が成り立つ.

ここで ab は G 内での a と b の積を表し, e は G の単位元を表す. $a \in G$ と $x \in X$ に対して組 (a, x) の写像 m による像を単に ax と書くことにすれば, 上の条件は全ての $a, b \in G$ と全ての $x \in X$ に対して $a(bx) = (ab)x$ 及び $ex = x$ が成り立つことである.

以下 G は X に作用する, 即ちこのような写像 $m : G \times X \to X$ が一つ与えられているものと仮定する. $a \in G$ に対して写像 $L_a : X \to X$ を $L_a(x) = ax$ で定義する.

補題 9.2. $L_a \in S_X$ である.

証明. $x, y \in X$ とせよ. $L_a(x) = L_a(y)$ ならば, $ax = ay$ であるから, $a^{-1}(ax) = a^{-1}(ay)$ 即ち, $(a^{-1}a)x = (a^{-1}a)y$. よって $ex = ey$ であり, 従って $x = y$ となり L_a は単射であることが分かる. また $L_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$ より $x = L_a(a^{-1}x)$ となり L_a が全射であることを得る. 故に $L_a \in S_X$ である. □

命題 9.3. 写像 : $G \to S_X$, $f(a) = L_a$ は準同型写像である.

証明. $a, b \in G$ とし $x \in X$ とすると, $f(ab)(x) = L_{ab}(x) = (ab)x = a(bx) = L_a(bx) = L_a(L_b(x)) = (L_aL_b)(x) = (f(a)f(b))(x)$ である. よって等式 $f(ab)(x) = (f(a)f(b))(x)$ が全ての $x \in X$ について成り立つので $f(ab) = f(a)f(b)$ である. 従って $f : G \to S_X$ は準同型写像である. □

定義と補題 9.4. 集合 X の上に関係 $\sim$ を

$$\sim = \{(x, y) \in X \times X \mid x = ay \text{ となる } G \text{ の元 } a \text{ が存在する } \}$$

によって定める. このとき $\sim$ は X 上の同値関係である.

証明. $x, y, z \in X$ とする. $x = ex$ であるから $x \sim x$ である. $x \sim y$ ならば, $x = ay$ となる $a \in G$ をとると, $a^{-1}x = a^{-1}(ay) = (a^{-1}a)x = ex = x$ より, $y \sim x$ であることが分かる. $x \sim y$ で $y \sim z$ なら $x = ay$, $y = bz$ $(a\ , b \in G)$ と書くと, $x = ay = a(bz) = (ab)z$ となり, $x \sim z$ であることが分かる. 従って関係 $\sim$ は集合 X 上の同値関係である. □

この関係 $\sim$ に関する $x \in X$ を含む同値類 $\mathrm{C}(x)$ は明らかに $\mathrm{C}(x) = \{ax \mid a \in G\}$ である. $\mathrm{C}(x)$ を x の G-**軌道** (the G-orbit of x) という. $x \in X$ に対して $N(x) = \{a \in G \mid ax = x\}$ と置き x における**等方群** (the isotropy group of x) という.

補題 9.5. $N(x)$ は G の部分群である.

証明. $e \in N(x)$ であるから $N(x)$ は空集合ではない. $a, b \in N(x)$ であれば, $bx = x$ より $b^{-1}x = b^{-1}(bx) = (b^{-1}b)x = ex = x$ である. 故に $b^{-1} \in N(x)$ である. 更に $(ab^{-1})x = a(b^{-1}x) = ax = x$ となり, $ab^{-1} \in N(x)$ を得る. 故に $N(x)$ は G の部分群である. □

命題 9.6. $|\mathrm{C}(x)| = [G : N(x)]$ である[26].

証明. 群 G 上に部分群 $N(x)$ が定める同値関係 R_1 を考え, 商集合 G/R_1 を作る. すると写像 $g : G \to \mathrm{C}(x)$, $g(a) = ax$ は全射であって, $\mathrm{R}_g = \mathrm{R}_1$ を満たすので系 2.7 より $|\mathrm{C}(x)| = [G : N(x)]$ が得られる. □

例題 9.7. 群 $GL(n, \boldsymbol{R})$ はベクトル空間 $\boldsymbol{R}^n$ に $m(A, \boldsymbol{x}) = A\boldsymbol{x}$ $(A \in GL(n, \boldsymbol{R}), \boldsymbol{x} \in \boldsymbol{R}^n)$ で作用する. この作用の軌道は $\boldsymbol{R}^n - \{\boldsymbol{o}\}$ と $\{\boldsymbol{o}\}$ の二つである.

証明. $A\boldsymbol{o} = \boldsymbol{o}$ $(^\forall A \in GL(n, \boldsymbol{R}))$ であるから, $\boldsymbol{o}$ を含む軌道は $\{\boldsymbol{o}\}$ である. 次に $\boldsymbol{x}$ を $\boldsymbol{o}$ と異なる任意のベクトルとする. $\boldsymbol{x}_1 = \boldsymbol{x}$ を補って $\boldsymbol{R}^n$ の基底 $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n$ を作ることが出来る. これらの (列) ベクトルを並べた行列を A とする. 即ち, $A = (\boldsymbol{x}_1\ \boldsymbol{x}_2\ \cdots\ \boldsymbol{x}_n)$ である. $\boldsymbol{e}_1$ を通常の様に, 第一成分が 1 で他の成分が 0 のベクトルとする. このとき, $A\boldsymbol{e}_1 = \boldsymbol{x}_1 = \boldsymbol{x}$ である. よって $\boldsymbol{e}_1$ の軌道は全ての $\boldsymbol{o}$ でないベクトルを含む. 即ち, $\boldsymbol{R}^n - \{\boldsymbol{o}\}$ である. □

例 9.8. 2 行 2 列の碁盤がある. この碁盤に黒石と白石を置くパターンが何通りあるか考えよう. 但し碁盤を回転して同じになる置き方は同じパターンと考える. 答えはすぐ分かるように, 全て黒石, 黒石三個で他は白石, 黒石が隣同士に二個で他は白石, 黒石が隣り合わない位置に二個で他は白石, 黒石一個で他は白石, 全て白石, の五つのパターンがある. 以上のパターンをそれぞれ (a), (b), (c), (d), (e), (f) と名付ける. この問題は次の様に考えられる. X を碁盤の回転を許さないで石を置く置き方の全体とする. X は $2^4 = 16$ 個の元からなる. 群 G を $G = \{e, a, a^2, a^3\}$ で定義する. 但し a は碁盤を $90°$ 回転する操作である. G は X に作用する. この問題は X を G による同値類に分類することと同じである. パターン (a), (b), (c), (d), (e), (f) の同値類はそれぞれ, 1, 4, 4, 2, 4, 1 個の元からなることは容易に分かるであろう.

有限集合 X に有限群 G が作用しているとする. このとき G の軌道の個数を与える公式を求めよう. 上の同値関係 $\sim$ に関する完全代表系を $a_1, a_2, \cdots, a_m$ とする. m が軌道 (同値類) の数である.

バーンサイドの定理 9.9. $g \in G$ に対して g が固定する x の個数, 即ち $gx = x$ である $x \in X$ の個数を $n(g)$ とする. このとき軌道の個数 m は

$$\frac{1}{|G|}\sum_{g \in G} n(g)$$

[26] 一方が有限ならば他方も有限で等しく, 一方が無限なら他方も無限であるという意味である.

に等しい.

証明. $F = \{(g, x) \in G \times X \mid gx = x\}$ とする. $\sum_{g \in G} n(g)$ は F の元を g ごとにまとめて数えたものだから $|F|$ に等しい. 逆に F の元を x ごとにまとめて数えると $\sum_{x \in X} |N(x)|$ に等しい. 即ち,

$$\sum_{g \in G} n(g) = \sum_{x \in X} |N(x)|$$

を得る. $N(ax) = aN(x)a^{-1} = \{aha^{-1} \mid h \in N(x)\}$ であるから $|N(ax)| = |N(x)|$ である. 上の式の右辺を同値なものごとにまとめて和を取ると

$$\begin{aligned}\sum_{x \in X} |N(x)| &= \sum_{i=1}^{m} \sum_{x \in \mathrm{C}(a_i)} |N(x)| \\ &= \sum_{i=1}^{m} \sum_{x \in \mathrm{C}(a_i)} |N(a_i)| \\ &= \sum_{i=1}^{m} |\mathrm{C}(a_i)| \cdot |N(a_i)|\end{aligned}$$

を得る. 命題 9.6 により $|\mathrm{C}(a_i)| \cdot |N(a_i)| = |G|$ であるから, 最後の和は $m|G|$ に等しい. よって定理は証明された. □

例 9.10. 例 9.8 を再び考えよう. e は全ての X の元を固定するから $n(e) = 16$ である. a, a^3 によって固定されるのは, 全てが黒石又は白石の場合であるから $n(a) = n(a^2) = 2$ である. a^2 によって固定されるのは, 隣り合わない位置に同じ色の石を置く場合であるから $n(a^2) = 4$ である. 従って軌道の個数は $(16 + 2 + 2 + 4)/4 = 6$.

例 9.11. 青, 赤, 白の椅子を合計 5 個円状に置く置き方の数を求めよう. X を椅子を円状に置く置き方の全体とする. 但しこの段階では椅子は固定されているものとする. X は $3^5 = 243$ 個の元からなる. a を椅子を $72°$ 回転する操作とする. $G = \{e, a, a^2, a^3, a^4\}$ が X に作用する. $n(e) = 243$ である. a で不変な椅子の置き方は全ての椅子が同じ色の場合であるから $n(a) = 3$ である. 同様に $n(a^2) = n(a^3) = n(a^4) = 3$ である. 従って軌道の個数は $(243 + 3 + 3 + 3 + 3)/5 = 51$.

例 9.12. 立方体の六面を異なる六色で塗る塗り方を考えよう. 但し各面は互いに異なる色で塗られるものとする. X を立方体を固定した状態で塗る塗り方の全体とする. $|X| = 6!$ である. G を正六面体群とする. $n(e) = 6!$ であり, $G \ni g \neq e$ のときは $n(g) = 0$ である. 従って塗り方の数は $6!/24 = 30$ 通りである.

問 9.1 G は群とし $X = G$ とする. 写像 $m_0, m_1 : G \times X \to X$ を $m_0(a, x) = ax$, $m_1(a, x) = axa^{-1}$ で定義する. m_0, m_1 は群の作用であることを確かめよ.

問 9.2　G は群とし X は空でない集合とする．次の主張を証明せよ．群 G の集合 X への作用 $m : G \times X \to X$ を一つ考えることと, 群 G から群 S_X への準同型写像 $f : G \to S_X$ を一つ考えることとは同値である．

問 9.3　$X = M_{m,n}(\boldsymbol{R})$ とし, $G = GL(m, \boldsymbol{R}) \times GL(n, \boldsymbol{R})$ とする．$(P, Q) \in G$, $M \in X$ に対して $m((P, Q), M) = PMQ^{-1}$ と置く．m は群 G の X への作用であることを確かめよ．この作用による X の同値類を求め標準的な代表系を求めよ．(正則行列は基本行列の積で表せる．両側から正則行列をかけることは基本変形をすることと同じであることを思い出せ.)

問 9.4^{ℓ}　立方体の六面を異なる 4 色 A, B, C, D で塗る．2 面を A, 2 面を B, 1 面を C, 1 面を D で塗る塗り方は何通りあるか.

問 9.5^{ℓ}[27]　赤い椅子五脚と白い椅子五脚の合計十脚を円状に並べる並べ方は何通りあるか.

問 9.6^{ℓ}　立方体の 8 頂点の中の 5 個を黒で 3 個を白で塗る塗り方は何通りあるか.

問 9.7^{ℓ}　4 行 4 列の碁盤がある．この碁盤に黒と白の石を置く置き方は何通りあるか.

§10　準同型写像と正規部分群 (homomorphism and normal subgroups)

G, G' は群で $f : G \to G'$ は準同型写像とする．従って f は群 G から群 G' への写像であって, G の全ての元 a, b について等式 $f(ab) = f(a)f(b)$ が成り立つ．勿論ここで ab は G 内での積を表し, $f(a)f(b)$ は G' 内での積を表している．

例 10.1.

1)　写像 $f : GL(n, \boldsymbol{R}) \to \boldsymbol{R}^*$, $f(A) = \det A$ は準同型写像である．

2)　$\mathrm{sgn} : S_n \to \boldsymbol{R}^*$, $s \mapsto \mathrm{sgn}(s)$ は準同型写像である．

3)　n 次元ベクトル空間 $\boldsymbol{R}^n$ から m 次元ベクトル空間 $\boldsymbol{R}^m$ への線形写像は, ベクトル空間の加法について準同型写像である．

4)　$\boldsymbol{R}$ から $\boldsymbol{R}^+ = \{a \in \boldsymbol{R} \mid a > 0\}$ への写像 $f : \boldsymbol{R} \to \boldsymbol{R}^+$, $f(x) = \exp(x)$ は同型写像である．

5)　写像 $f : \boldsymbol{R} \to GL(2, \boldsymbol{R})$ を $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ によって定義すれば f は準同型写像である．

6)　a を群 G の元とし写像 $f : \boldsymbol{Z} \to G$ を $f(n) = a^n$ と定義すれば, f は準同型写像となる．

7)　a を群 G の元とし写像 $i_a : G \to G$ を $i_a(x) = axa^{-1}$ と定義すれば, i_a は G から G 自身への同型写像となる．

8)　群 G から群 S_G への写像 $f : G \to S_G$, $f(a) = i_a$ は準同型写像である．

9)　群 G から群 S_G への写像 $f : G \to S_G$, $f(a) = L_a$ は準同型写像である．

[27] 1994 年日本数学オリンピック予選問題 (対馬出題).

補題 10.2.

1) $a_1, a_2, \cdots, a_n$ が G の元であれば $f(a_1a_2\cdots a_n) = f(a_1)f(a_2)\cdots f(a_n)$ が成り立つ.

2) n を整数とし a を G の元とすれば $f(a^n) = f(a)^n$ である. 特に $f(e) = e'$, $f(a^{-1}) = f(a)^{-1}$ である. 但し e は G の単位元で e' は G' の単位元である.

証明. 1) $n = 2$ のときは準同型写像の定義に従うから, $n \geqq 3$ で $n-1$ までは主張は成り立つとしてよい. すると $a_1a_2\cdots a_n = (a_1\cdots a_{n-1})a_n$ であるから, $f(a_1a_2\cdots a_n) = f((a_1\cdots a_{n-1})a_n) = f(a_1\cdots a_{n-1})f(a_n) = (f(a_1)\cdots f(a_{n-1}))f(a_n) = f(a_1)f(a_2)\cdots f(a_n)$ である.

2) $f(e) = f(e^2) = f(e)^2$ であるから, 補題 6.1 の 4) より $f(e) = e'$ を得る. $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ であるから, 補題 6.1 の 5) より $f(a^{-1}) = f(a)^{-1}$ である. $f(a^n) = f(a)^n$ であることは n が自然数のときは 1) に従う. n が負のときは $a^n = (a^{-1})^{-n}$ であるから, $f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^{-n} = f(a)^n$ となる. □

命題 10.3.

1) H が G の部分群であれば, $f(H) = \{f(h) \mid h \in H\}$ は G' の部分群である.

2) H' が G' の部分群であれば, $f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$ は G の部分群である.

証明. 1) $f(H)$ は G' の空でない部分集合である. a', b' を $f(H)$ の元とすれば, $a' = f(a)$, $b' = f(b)$ となる G の元 a, b を取れる. $a'(b')^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ であって, H は G の部分群であるから, 定義と定理 8.1 より ab^{-1} は H の元である. よって $a'(b')^{-1}$ は H' の元であって, H' が G' の部分群であることが分かる.

2) $f(e) = e'$ で e' は H' に含まれているから, e は $f^{-1}(H')$ に含まれる. 従って $f^{-1}(H')$ は G の空でない部分集合である. a, b を $f^{-1}(H')$ の元とすると, $f(ab^{-1}) = f(a)f(bb^{-1}) = f(a)f(b)^{-1}$ であって, $f(a)$, $f(b)$ は H' の元であるから, $f(a)f(b)^{-1}$ は H' に含まれ, 従って ab^{-1} は $f^{-1}(H')$ の元である. □

定義 10.4.

1) $\mathrm{Ker}\, f = \{a \in G \mid f(a) = e'\}$ と置き f の**核** (the kernel of f) という. $\mathrm{Ker}\, f = f^{-1}(e')$ であるから $\mathrm{Ker}\, f$ は G の部分群である.

2) $\mathrm{Im}\, f = f(G) = \{f(a) \mid a \in G\}$ と置き f の**像** (the image of f) という. $\mathrm{Im}\, f$ は G' の部分群である.

命題 10.5. G がアーベル群であれば $\mathrm{Im}\, f$ はアーベル群である.

証明. a', b' を $\mathrm{Im}\, f$ の元とし, $a' = f(a)$, $b' = f(b)$ である G の元 a, b を取る. すると $a'b' = f(a)f(b) = f(ab)$ であって, $b'a' = f(b)f(a) = f(ba)$ である. 従って G がアーベル群ならば $\mathrm{Im}\, f$ もアーベル群である. □

定義と命題 10.6. N は G の部分群とする. N が次の条件

$$\underline{G \text{ の全ての元 } a \text{ について } aN = Na \text{ である}}$$

を満たすとき, N は G の**正規部分群** (a normal subgroup of G) であるという. この条件は

$$\underline{G \text{ の全ての元 } a \text{ について } aNa^{-1} = \{ana^{-1} \mid n \in N\} \text{ が } N \text{ に含まれる}}$$

ことと同値である.

証明. a を G の元, n を N の元とする. N が G の正規部分群であれば, $aN = Na$ であって, ある N の元 n_1 によって $an = n_1a$ と表され, 従って $ana^{-1} = n_1$ で aNa^{-1} は N に含まれることが分かる. 逆に G の全ての元 b について $bNb^{-1} = \{bnb^{-1} \mid n \in N\}$ が N に含まれるならば, ana^{-1} は N の元であるから, $n_1 = ana^{-1}$ と置くと, $an = n_1a$ となり, an が Na の元であって, aN は Na の部分集合であることが分かる. 同様に $n_2 = a^{-1}n(a^{-1})^{-1} = a^{-1}na$ は N の元であるから $na = an_2$ より, na は aN の元であって, Na が aN の部分集合であることが得られ, $aN = Na$ となる. □

$f : G \to G'$ を準同型写像とする. $K = \mathrm{Ker}\, f$ と置く.

命題 10.7. K は G の正規部分群である.

証明. k を K の元とすると, G の元 a について $f(aka^{-1}) = f(a)f(k)f(a^{-1}) = f(a)e'f(a)^{-1} = e'$ である. 即ち, aka^{-1} は K の元であるよって. 定義と命題 10.6 に従う. □

命題 10.8. N が G の部分群で $[G : N] = 2$ あれば, N は G の正規部分群である.

証明. a が N の元であれば $aN = Na = N$ である. a を G の元で N には含まれないものとすれば, $aN \neq N$, $Na \neq N$ である. 一方 $aN = G - N$, $Na = G - N$ であるから, 結局 $aN = Na$ となり N が G の正規部分群であることが分かる. □

補題 10.9. 次の 2 条件は同値である.

1) $K = \{e\}$ である.

2) f は単射である.

このとき群 G と群 $\mathrm{Im}\, f$ とは同型である.

証明. $f(a) = f(b)$ なら $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e$ であるから, ab^{-1} は K の元である. よって 1) から 2) が得られる. 2) から 1) が得られることは明らかであろう. f が単射ののときは写像 $f' : f \to \mathrm{Im}\, f$ を $f'(a) = f(a)$ によって定めれば, f' は全単射であるから同型写像である. □

次の定理は有限群論における対称群研究の重要性を示していると考えられる.

定理 10.10. G を元の個数が n の有限群とすれば, G は対称群 S_n の部分群と同型である.

証明. 定理 6.5 と補題 10.9 に従う. □

問 10.1　例 10.1 内の写像が準同型写像であることを確かめよ.

問 10.2　G がアーベル群であれば全ての部分群は正規部分群であることを示せ.

問 10.3　$SL(n, \boldsymbol{R})$ は $GL(n, \boldsymbol{R})$ の正規部分群であることを確かめよ.

問 10.4　A_n は S_n の正規部分群であることを確かめよ.

問 10.5　S_3 と S_4 の正規部分群を全て書き出せ.

問 10.6　問 8.5 の群 G 内では全ての部分群が正規部分群となっていることを確かめよ[28].

問 10.7*　次の主張を証明せよ.

1)　f が全射であってかつ N が G の正規部分群であれば, $N' = f(N)$ は G' の正規部分群である.

2)　N' が G' の正規部分群であれば, $N = f^{-1}(N')$ は G の正規部分群である.

問 10.8　H は G の部分群とする. 次の主張を証明せよ.

1)　G の元 a に対して $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ と置けば aHa^{-1} は G の部分群である.

2)　H が G の正規部分群であるための必要かつ十分な条件は, G の全ての元 a について $aHa^{-1} = H$ となることである.

3)　G は有限群とせよ. H と同じ位数を持つ部分群が G 内には H の他に含まれていないならば H は G の正規部分群である.

§11　巡回群 (cyclic groups)

G は群とする. G の元 a に対して $\langle a \rangle = \{a^n \mid n \in \boldsymbol{Z}\}$ と置き, 元 a で**生成された** G の部分群という. もし G がアーベル群でその演算が加法で表示されているときは, 勿論 $\langle a \rangle = \{na \mid n \in \boldsymbol{Z}\}$ である. 群 G が巡回群であるとは, $G = \langle a \rangle$ となる元 a が G 内に少なくとも一つは含まれていることをいう. 例えば加法群 $\boldsymbol{Z}$ は 1 で生成された最も基本的は巡回群である. 群 G が元 a で生成された巡回群であれば, 準同型写像 $f : \boldsymbol{Z} \to G$, $f(n) = a^n$ は全射であり, $\boldsymbol{Z}$ はアーベル群であるから, 命題 10.5 より全ての巡回群はアーベル群であることが分かる.

例 11.1.　n は自然数とし $C_n = \{z \in \boldsymbol{C} \mid z^n = 1\}$ と置けば, C_n は位数 n の巡回群である (問 11.1).

例 11.2.　S_n 内で巡回置換 $s = (1, 2, 3, \cdots, n-1, n)$ を考え $H_n = \langle s \rangle$ とすれば, H_n は位数 n の巡回群である (問 11.2).

次の節で示すように, 巡回群は全て $\boldsymbol{Z}$ 又は C_n (n は自然数) に同型である. 従って位数の等しい二つの巡回群は互いに同型になる. 例えば例 11.1 の C_n と例 11.2 の H_n は同型である.

[28] この例より全ての部分群が正規部分群であっても G はアーベル群とは限らないことが分かる.

定理 11.3. 巡回群の部分群は全て巡回群である.

証明. H を元 a で生成された巡回群 G の部分群とする. $H = \{e\}$ であれば $H = \langle e \rangle$ であるから, 以後は $H \neq \{e\}$ と仮定しよう. すると元 b で $b \neq e$ であるものが H 内に存在する. b は G の元であるから, $b = a^n$ の形に表すことができる. ここで $n \neq 0$ であるが $n < 0$ であるかも知れない. もし $n < 0$ であれば, $b^{-1} = a^{-n}$ であって $-n$ は正であり, 勿論 b^{-1} は H の元でである. 従って必要ならば b の代わりに b^{-1} を考えることにより, $n > 0$ であると仮定することができる. 従って $a^n \in H$ を満たす自然数 n が存在する. このような自然数の内で最小のものを取りそれを改めて n と置く. すると $H = \langle a^n \rangle$ となる. 実際 $h \in H$ とすれば, $h = a^m$ (m は整数) と表されるが, ここで $m = nq + r$ ($0 \leqq r < n$) となる整数 q, r を取ると, $h = a^m = a^{nq}a^r$ であって $a^r = h(a^n)^{-q}$ である. h, a^n はどちらも H の元であったから, $a^r = h(a^n)^{-q}$ は H の元であって, n の最小性より $r = 0$ でなければならない. よって $h = (a^n)^q$ となり H が $\langle a^n \rangle$ に含まれることが分かる. 勿論 $\langle a^n \rangle$ は H の部分集合であるから $H = \langle a^n \rangle$ である. □

系 11.4. 加法群 $\boldsymbol{Z}$ の部分群は全て巡回群である.

定義 11.5. 群 G の元 a に対して部分群 $\langle a \rangle$ の元の個数 (即ち群 $\langle a \rangle$ の位数) を a の**位数** (the order of a) と呼び $o(a)$ と書く. $o(a)$ は自然数か又は ∞ である.

例えば $G = \boldsymbol{Z}$ としと $a = 1$ すれば $\langle a \rangle = \boldsymbol{Z}$ だから $o(1) = \infty$ である. $G = S_3$ とし $s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $(= (1,2,3))$ とすれば $\langle s \rangle = \{e, s, s^2\}$ であって $o(s) = 3$ となる.

定理 11.6. a は群 G の元とする. 次の 2 条件は同値である.

1) $o(a)$ は有限である.

2) $a^m = e$ となる自然数 m が少なくとも一つ存在する.

このとき等式 $o(a) = \min\{m \in \boldsymbol{N} \mid a^m = e\}$ が成り立ち, 更に $n = o(a)$ と置くと $\langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$ となる.

証明. 写像 $f : \boldsymbol{Z} \to G$ を $f(m) = a^m$ で定義すると, f は準同型写像であって, $\operatorname{Im} f = \langle a \rangle$ である. $K = \operatorname{Ker} f$ と置く. K は $\boldsymbol{Z}$ の部分群であるから, 系 11.4 より $K = \langle n \rangle$ となる非負整数 n を取れる. $n > 0$ と仮定する. 任意の整数 m に対して $m = nq + r$ ($0 \leqq r < n$) と置くと, $a^m = (a^n)^q a^r = a^r$ となるから $\langle a \rangle = \{a^r \mid 0 \leqq r < n\}$ である. ここでもし $a^r = a^s$ ($0 \leqq r < s < n$) であれば, $a^{s-r} = e$ となるから $s - r$ は K の元であり, 従って n の倍数でなければならないが, これは r, s が $0 \leqq r < s < n$ を満たす以上あり得ない. よって $o(a) = n$ であり n は $a^n = e$ である最小の自然数である. 二つの条件が同値であることを証明しよう. $o(a)$ が有限であれば, f は単射ではあり得ないから, $K \neq \{0\}$ で従って $n > 0$ であり $a^n = e$ である. 逆に $a^m = e$ である自然数 m が少なくとも一つ存在したと仮定しよう. このとき m は K の元であるから, $n > 0$ となり上に示したように, $n = o(a)$ で確かに $o(a)$ は有限である. □

系 11.7. $o(a)$ が有限であれば, 整数 m について $a^m = e$ となるための必要かつ十分な条件は, $o(a)$ が m を割り切ることである.

証明. 定理 11.6 の証明に従う. □

系 11.8. G は有限群とし G の位数を n とすると, G の全ての元 a に対して $a^n = e$ となる.

証明. G は有限群であるから $o(a)$ は有限である. 一方 Cauchy の定理 8.7 より $o(a)$ は n を割り切る. 定理 11.6 より $a^{o(a)} = e$ であるから $a^n = e$ である. □

例題 11.9. $o(a) = n$ が有限であれば, 任意の整数 m について等式 $o(a^m) = n/(m,n)$ が成り立つ. 但し (m,n) は m と n の最大公約数を表す. 特に $(m,n) = 1$ であれば $o(a^m) = n$ である.

証明. $(m,n) = s$ と置き $m = sm'$, $n = sn'$ と書いておく. $(a^m) = r$ とせよ. すると $a^{mr} = (a^m)^r = e$ であるから, 系 11.7 により n は mr を割り切る. 即ち, n' は $m'r$ を割る. $(m',n') = 1$ であるから, n' は r を割り切る. 逆に $(a^m)^{n'} = a^{mn'} = a^{sn'm'} = (a^n)^{m'} = e$ となり, 系 11.7 により r は n' を割り切る. よって $r = n' = n/(m,n)$ である. □

定理 11.10. G は有限巡回群とし $|G| = n$ とする. m を n の約数とせよ. このとき位数が m であるような部分群 H が G 内に唯一つだけ含まれている.

証明. $G = \langle a \rangle$ とする. 勿論 $o(a) = n$ である. m を n の約数とし $n = mk$ と書き, $H = \langle a^k \rangle$ と置く. 例題 11.9 より $|H| = o(a^k) = n/(n,k) = n/k = m$ となる. 従って位数 m の部分群は確かに存在する. さて H は G の部分群で位数が m のものとせよ. すると系 11.8 より H は集合 $H_m = \{x \in G \mid x^m = e\}$ に含まれる. G はアーベル群であるから, すぐ分かるように H_m は G の部分群である. 定理 11.3 より H_m は巡回群であるから, $H_m = \langle b \rangle$ となるような元 b が G 内に存在する. $b^m = e$ であるから $o(b)$ は m 以下であり, 従って H_m の元の個数は高々 m である. H は位数 m であって H_m は H を含むから, 結局 $H = H_m$ となる. よって一意性を得る (H_m は m のみによって定義されている). □

例題 11.11. H, K を有限巡回群 G の部分群とする. このとき H が K に含まれるための必要かつ十分な条件は, $|H|$ が $|K|$ の約数であることである.

証明. $H \subset K$ であれば $|H|$ が $|K|$ を割り切ることは, Cauchy の定理 8.7 による. $|H| = m$, $|K| = n$ と置き, $m \mid n$ と仮定しよう. すると $m \mid n$ より有限巡回群 K 内には位数が m の部分群が唯一つ存在する. それを H' とすれば, H も H' もどちらも G の部分群であって同じ位数を持つから, 定理 11.10 より $H = H'$ でなければならない. 従って H は K に含まれる. □

問 11.1　例 11.1 を確かめよ.

問 11.2　例 11.2 を確かめよ.

問 11.3 〜問 11.7　次の集合 H は $\boldsymbol{Z}$ の部分群であることを示し, $H = \langle a \rangle$ となる $\boldsymbol{Z}$ の元 $a \geqq 1$ を求めよ.

問 11.3^m　$H = \{3x + 7y \mid x, y \in \boldsymbol{Z}\}$.

問 11.4^m　$H_1 = \{12x + 42y \mid x, y \in \boldsymbol{Z}\}$.

問 11.5^m　$H = \{12x + 42y + 5z \mid x, y, z \in \boldsymbol{Z}\}$.

問 11.6^m　$H_2 = \{16x + 24y \mid x, y \in \boldsymbol{Z}\}$.

問 11.7^m　H は H_1 と H_2 の共通部分.

問 11.8　S_3 と S_4 の元の位数を全て計算せよ.

問 11.9^*　G は $\boldsymbol{C}^*$ の部分群とする. $|G| = n < \infty$ なら $G = C_n$ であることを証明せよ.

問 11.10　位数 24, 36, 49 の巡回群の部分群を全て書き出し, その包含関係を図示せよ.

問 11.11^*　G は群で $G \neq \{e\}$ なるものとする. 次の主張を証明せよ. G が G 自身と $\{e\}$ の他に部分群を含まないために必要かつ十分な条件は, G は有限群でしかも G の位数が素数であることである.

問 11.12^*　$s, t \in S_n$ が同じ文字を含まないとする. このとき s, t の位数を k, l とすれば, st の位数は k と l の最小公倍数である (命題 7.8 を使う).

§12　剰余類群と同型定理 (factor groups and isomorphism theorems)

G を群とし N を G の正規部分群とする. すると G の全ての元 a について $aN = Na$ であるから, G 上に N の定める二つの同値関係 R_1 と R_2 は実は同じものである. 商集合 $G/\mathrm{R}_1 = G/\mathrm{R}_2$ を単に G/N と書く. このとき G/N は次の演算によって群となる:

$$aN \circ bN = (ab)N.$$

この群を G の N による**剰余類群** (the factor group of G by N) と呼ぶ. 自然な写像 $f : G \to G/N$, $f(a) = aN$ は準同型写像であって, $\mathrm{Ker}\, f = N$ が成り立つ. 勿論 f は全射である. なお G/N 内の単位元は $eN = N$ であって, $(aN)^{-1} = a^{-1}N$ であることに注意せよ.

定理 12.1.　$g : G \to G'$ を群の準同型写像とし, N を G の正規部分群で $\mathrm{Ker}\, g$ に含まれるものと仮定する. このとき準同型写像 $h : G/N \to G'$ で G の全ての元 a について $h(aN) = g(a)$ を満たすものが唯一つ存在する.

証明.　$f : G \to G/N$, $f(a) = aN$ とする. a, b を G の元とせよ. もし $aN = bN$ ならば, $a^{-1}b \in N$ より $a^{-1}b$ は $\mathrm{Ker}\, g$ に含まれる. 従って $g(a^{-1}b) = e$ だから, $g(a) = g(b)$ が得られる. 故に定理 2.5 よ

り, 写像 $h : G/N \to G'$ で G の全ての元 a について $h(aN) = g(a)$ を満たすものが唯一つ存在する. この写像 h が準同型写像であることは, $h(aN \circ bN) = h((ab)N) = g(ab) = g(a)g(b) = h(aN)h(bN)$ に従う. □

系 12.2[29]**.** $g : G \to G'$ を群の準同型写像とし, $K = \operatorname{Ker} g$ と置く. このとき単射準同写像 $h : G/K \to G'$ であって, G の全ての元 a について $h(aK) = g(a)$ を満たすものが唯一つ存在する. 特に G/K は $\operatorname{Im} g$ と同型である.

証明. 定理 12.1 によって, 準同型写像 $h : G/K \to G'$ で G の全ての元 a について, $h(aK) = g(a)$ を満たすものが唯一つ存在する. 元 a, b が G の元であれば, $g(a) = g(b)$ であるための必要十分条件は $a^{-1}b \in K$ であるから, この h は定理 2.5 の 3) によって単射である. 補題 10.9 より G/K は $\operatorname{Im} h = \operatorname{Im} g$ と同型である. □

系 12.3. 位数の等しい二つの巡回群は互いに同型である.

証明. G を巡回群で $|G| = n$ なるものとし, $G = \langle a \rangle$ とする. 写像 $f : \boldsymbol{Z} \to G$ を $f(m) = a^m$ で定め, $\operatorname{Ker} f = N$ と置く. するともし $o(a) = \infty$ ならば, 定理 11.6 より $N = \{0\}$ であって, 従って系 12.2 より $\boldsymbol{Z}$ と G とは同型である. $n = o(a) < \infty$ とする. このとき, 系 11.7 より $N = \langle n \rangle$ であって, 従って系 12.2 より $\boldsymbol{Z}/\langle n \rangle$ と G とは同型である. □

系 12.4[30]**.** $g : G \to G'$ を群の準同型写像で全射であるとせよ. N' を G' の正規部分群とし $N = g^{-1}(N')$ と置く. 問 10.7 の 1) により N は G の正規部分群である. このとき群 G/N と G'/N' とは同型である.

証明. 準同型写像 $g : G \to G'$ と自然な準同型写像 $f : G' \to G'/N'$ を合成して準同型写像 $h = f \circ g : G \to G'/N'$ を作ると, h は準同型写像で全射である. $\operatorname{Ker} h = N$ であるから, 系 12.2 によって G/N と G'/N' とは同型である. □

補題 12.5. H, K は群 G の部分群とし, $HK = \{hk \mid h \in H, k \in K\}$ と置く. このとき集合 HK が G の部分群であるための必要かつ十分な条件は, $HK = KH$ が成り立つことである.

証明. HK が G の部分群であると仮定せよ. このとき $h \in H$, $k \in K$ とすると $(hk)^{-1} \in HK$ であるから, ある $h_1 \in H$, $k_1 \in K$ が存在して $(hk)^{-1} = h_1k_1$ と表すことができる. 従って $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$ を得る. 故に HK は KH の部分集合である. $(kh)^{-1} = h^{-1}k^{-1}$ より $(kh)^{-1} \in HK$ である. 故に $kh = ((kh)^{-1})^{-1} \in HK$ を得る. 即ち KH は HK の部分集合であり, 従って $HK = KH$ となる. 逆に $HK = KH$ と仮定せよ. h, $h_1 \in H$ とし k, $k_1 \in K$ とすると, $(hk)(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1}$ であって, $kk_1^{-1}h_1^{-1} \in KH = HK$ より $kk_1^{-1}h_1^{-1} = h_2k_2$ $(h_2 \in H,\ k_2 \in K)$ と書くことができる. 従って $(hk)(h_1k_1)^{-1} = hh_2k_2 \in HK$ となって, HK が G の部分群であることが分かる. □

[29]準同型定理という.
[30]第一同型定理という.

系 12.6. N, H は群 G の部分群とする. もし N が G の正規部分群であれば, 集合 NH は必ず G の部分群である.

証明. NH は集合 Nh $(h \in H)$ の和集合であって, HN は hN $(h \in H)$ の和集合である. $hN = Nh$ であるから $HN = NH$ となる. 故に補題 12.5 より NH は G の部分群である. □

系 12.7[31]**.** N, H は群 G の部分群で, N は G の正規部分群であると仮定する. $H \cap N$ は H の正規部分群, N は NH の正規部分群であって, しかも $H/H \cap N$ と NH/N は同型である.

証明. 勿論 N は NH の正規部分群であって, 準同型写像 $f : H \to NH/N$, $f(h) = hN$ の核は $H \cap N$ である. よって命題 10.7 より $H \cap N$ は H の正規部分群である. 一方 $n \in N$, $h \in H$ とすると, $(nh)N = N(nh) = Nh = hN$ であるから f は全射である. よって系 12.2 により $H/H \cap N$ と NH/N とは同型である. □

剰余類群がアーベル群になるための条件を与えておく.

定義と命題 12.8. a, b を群 G の元とする. $[a, b] = aba^{-1}b^{-1}$ と置いて a, b の**交換子**と呼ぶ. G の有限個の交換子の積の全体を $[G, G]$ で表す. $[G, G]$ は G の部分群である. これを G の**交換子群**と呼ぶ.

証明. $g, h \in [G, G]$ とする. $g = [a_1, b_1] \cdots [a_m, b_m]$, $h = [c_1, d_1] \cdots [c_n, d_n]$ と表せる. $[c_i, d_i]^{-1} = (c_i d_i c_i^{-1} d_i^{-1})^{-1} = d_i c_i d_i^{-1} c_i^{-1} = [d_i, c_i]$ である. よって $gh^{-1} = [a_1, b_1] \cdots [a_m, b_m] ([c_1, d_1] \cdots [c_n, d_n])^{-1} = [a_1, b_1] \cdots [a_m, b_m][c_n, d_n]^{-1} \cdots [c_1, d_1]^{-1} = [a_1, b_1] \cdots [a_m, b_m][d_n, c_n] \cdots [d_1, c_1]$ であるから $gh^{-1} \in [G, G]$ である. □

定理 12.9. H を群 G の部分群とする. H が G の正規部分群でかつ G/H がアーベル群であるための必要十分条件は, H が G の交換子群 $[G, G]$ を含むことである. 特に交換子群 $[G, G]$ は正規部分群である.

証明. H が G の正規部分群で, G/H がアーベル群であるとする. $A = aH$, $B = bH$ を G/H の任意の元とするとき, $AB = BA$ であるから, $ABA^{-1}B^{-1}$ は G/H の単位元 H に等しい. よって $ABA^{-1}B^{-1} = aba^{-1}b^{-1}H = H$ である. 従って $[a, b] = aba^{-1}b^{-1} \in H$. 全ての交換子が H に含まれるから, それらの積全体である $[G, G]$ は H に含まれる.

逆に, H を G の部分群として $H \supset [G, G]$ と仮定する. $a \in H$, $t \in G$ に対して $tat^{-1} = tat^{-1}a^{-1}a = [t, a]a \in [G, G]a \subset H$ であるから, H は正規部分群である. $ab = ba(a^{-1}b^{-1}ab) = ba[a^{-1}, b^{-1}]$ で $[a^{-1}, b^{-1}] \in [G, G] \subset H$ であるから

$$abH = ba[a^{-1}, b^{-1}]H = baH.$$

[31]第二同型定理という.

従って, $A = aH$, $B = bH$ と置くと $AB = aHbH = abH = baH = bHaH = BA$ となり, G/H はアーベル群である. □

問題 12.1　N を群 G の正規部分群とする. このとき, G/N が群になることを確かめよ. 特にどこに N が G の正規部分群であることを用いているかを明確に述べよ.

問題 12.2　群 $GL(n, \boldsymbol{R})/SL(n, \boldsymbol{R})$ と群 $\boldsymbol{R}^*$ とは同型であることを確かめよ.

問題 12.3[32]　N は群 G の正規部分群として $G' = G/N$ と置く. このとき集合 $\{H \mid H$ は G の部分群で N を含む $\}$ と集合 $\{H' \mid H'$ は G' の部分群である $\}$ との間には, 自然な一対一かつ上への対応 $H \to H' = H/N$ が存在し, この対応によって正規部分群は正規部分群に対応していることを証明せよ. 対応する正規部分群による剰余類群は互いに同型であることを確かめよ.

問 12.4　対称群 S_3, S_4 の交換子群を求めよ. (交換子は偶置換であることに注意せよ.)

§13　有限生成アーベル群

この節では群は全てアーベル群であると仮定し, 演算は加法で表されているとする.

定義 13.1.　群 G の元 $a_1, a_2, \cdots, a_n$ が存在して, G の任意の元 a が

$$a = m_1a_1 + m_2a_2 + \cdots + m_na_n \quad (m_1,\ m_2,\ \cdots,\ m_n \in \boldsymbol{Z})$$

と表せるとき, G を**有限生成**アーベル群と言い, $a_1, a_2, \cdots, a_n$ を G の**生成元**と言う.

定義と命題 13.2.　$a_1, a_2, \cdots, a_n \in G$ とする. G の任意の元 a が一意的に

$$a = m_1a_1 + m_2a_2 + \cdots + m_na_n \quad (m_1,\ m_2,\ \cdots,\ m_n \in \boldsymbol{Z})$$

の形に表せるとき, G を**階数 n の自由アーベル群**と言い, $a_1, a_2, \cdots, a_n$ を G の**基底**と言う. $a_1, a_2, \cdots, a_n$ を生成元とする有限生成アーベル群 G が, $a_1, a_2, \cdots, a_n$ を基底とする自由アーベル群であるための必要十分条件は, 次の条件が成り立つことである. 但し, 整数 0 と区別するために G の単位元を 0_G で表している.

$$m_1a_1 + m_2a_2 + \cdots + m_na_n = 0_G \text{ ならば, } m_1 = m_2 = \cdots = m_n = 0.$$

証明.　G が自由アーベル群とする. もし

$$m_1a_1 + m_2a_2 + \cdots + m_na_n = 0_G = 0a_1 + 0a_2 + \cdots + 0a_n$$

[32] この結果を対応定理と呼ぶ.

ならば, 表し方の一意性により $m_1 = m_2 = \cdots = m_n = 0$ である. 逆に上の条件が成り立つとする. G の元 a が二通りの方法で表せたとする. 即ち,

$$a = m_1a_1 + m_2a_2 + \cdots + m_na_n = m_1'a_1 + m_2'a_2 + \cdots + m_n'a_n$$

とする. このとき

$$(m_1 - m_1')a_1 + (m_2 - m_2')a_2 + \cdots + (m_n - m_n')a_n = 0_G$$

が成り立つ. (以上の変形において交換法則を使っていることに注意せよ.) 従って, 上の条件より $m_1 = m_1'$, $m_2 = m_2'$, $\cdots$, $m_n = m_n'$ となって, a の表し方は一意的である. □

例 13.3. V を $\boldsymbol{R}$ 上の n 次元ベクトル空間として, $\boldsymbol{x}_1$, $\boldsymbol{x}_2$, $\cdots$, $\boldsymbol{x}_n$ を一つの基底とする. このとき

$$G = \{m_1\boldsymbol{x}_1 + m_2\boldsymbol{x}_2 + \cdots + m_n\boldsymbol{x}_n \mid m_1,\ m_2,\ \cdots,\ m_n \in \boldsymbol{Z}\}$$

は階数 n の自由アーベル群である.

自由アーベル群 G の元 $a = m_1a_1 + m_2a_2 + \cdots + m_na_n$ に対して, $\boldsymbol{Z}$ の n 個の直積 $\boldsymbol{Z}^n = \boldsymbol{Z} \times \boldsymbol{Z} \times \cdots \times \boldsymbol{Z}$ の元 $(m_1, m_2, \cdots, m_n)$ を対応させる写像は明らかに同型写像である. しかし, G の基底は唯一ではなく, 基底を取り替えれば[33] G と $\boldsymbol{Z}^n$ の間の同型写像が違ったものになることは, ベクトル空間の場合と同じである.

例題 13.4. G を自由アーベル群として, a_1, a_2, $\cdots$, a_n をその基底とする. b_1, b_2, $\cdots$, $b_n \in G$ とする. 各 b_i は

$$b_i = \sum_{j=1}^{n} c_{ij}a_j, \quad c_{ij} \in \boldsymbol{Z}$$

と表せる. b_1, b_2, $\cdots$, b_n が G の基底であるための必要十分条件は, 行列式 $|c_{ij}|$ が ± 1 に等しいことである.

証明. b_1, b_2, $\cdots$, b_n を G の基底と仮定する. 各 a_i は

$$a_i = \sum_{k=1}^{n} d_{ik}b_k, \quad d_{ik} \in \boldsymbol{Z}$$

と表せる. 右辺の b_k を a_1, a_2, $\cdots$, a_n で表して,

$$a_i = \sum_{k=1}^{n}\sum_{j=1}^{n} d_{ik}c_{kj}a_j = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} d_{ik}c_{kj}\right)a_j$$

が成り立つ. a_1, a_2, $\cdots$, a_n の和で表す仕方は唯一であるから,

$$\sum_{k=1}^{n} d_{ik}c_{kj} = \begin{cases} 1 & (i = j \text{ のとき}), \\ 0 & (i \neq j \text{ のとき}), \end{cases}$$

[33] 全ての G の基底は n 個の元からなることが証明できる. 問 13.4 参照.

である. 即ち, $D=(d_{ij})$, $C=(c_{ij})$ と置くと $DC=E$ である. $|D|\cdot|C|=|E|=1$ で $|D|$, $|C|$ は整数であるから, $|C|=\pm 1$ である.

逆に $|C|=\pm 1$ と仮定する. このとき $D=C^{-1}$ を C の余因子行列と $|C|$ で表す定理により, D の成分 d_{ij} は整数である.

$$\sum_{k=1}^{n} d_{ik}b_k=\sum_{k=1}^{n}\sum_{j=1}^{n} d_{ik}c_{kj}a_j=a_i$$

が成り立つ. よって a_i $(1\leqq i\leqq n)$ は b_j $(1\leqq j\leqq n)$ の整数係数の線形和で表せる. G の任意の元は a_i $(1\leqq i\leqq n)$ の整数係数の線形和で表せるので, 従って b_j $(1\leqq j\leqq n)$ の整数係数の線形和で表せる. 次に

$$\sum_{i=1}^{n} m_ib_i=m_1b_1+m_2b_2+\cdots+m_nb_n=0_G$$

である整数 m_i $(1\leqq i\leqq n)$ が存在すると,

$$\sum_{i=1}^{n} m_ib_i=\sum_{i=1}^{n}\sum_{j=1}^{n} m_ic_{ij}a_j=0_G=0a_1+0a_2+\cdots+0a_n$$

が成り立つ. a_j $(1\leqq j\leqq n)$ は基底であるから,

$$\sum_{i=1}^{n} m_ic_{ij}=0\quad(1\leqq j\leqq n)$$

を得る. 即ち,

$$(m_1,m_2,\cdots,m_n)(c_{ij})=(0,0,\cdots,0)$$

である. 従って $m_1=m_2=\cdots=m_n=0$ である. よって b_1, b_2, $\cdots$, b_n は G の基底である. □

定理 13.5. G を階数 n の自由アーベル群として, H を $\{0_G\}$ と異なる G の部分群とする. H は自由アーベル群であり, その階数 t は n を越えない. 更に, G の基底 u_1, u_2, $\cdots$, u_n を適当に選んで, c_1u_1, c_2u_2, $\cdots$, c_tu_t が H の基底であるように出来る. ここで, c_1, c_2, $\cdots$, c_t は正の整数で, c_i は c_{i+1} の約数である.

証明. n に関する帰納法による. $n=1$ の場合は系 11.4 による. 次に, G の階数が $n-1$ 以下の場合は定理が成り立つものとする. a_1, a_2, $\cdots$, a_n を G の基底として, H の各元 h を

$$h=m_1a_1+m_2a_2+\cdots+m_na_n\quad(m_1,\ m_2,\ \cdots,\ m_n\in\boldsymbol{Z})$$

として表す. $h\neq 0_G$ のとき $|m_i|$ $(1\leqq i\leqq n)$ の中の 0 でない最小の値を $m(h)$ とする. h が全ての $H-\{0_G\}$ の元を動くときの, $m(h)$ の最小値を H に関する基底 a_1, a_2, $\cdots$, a_n の大きさと呼ぶ. G の基底の中で大きさが最小のものをとり, b_1, b_2, $\cdots$, b_n とし, その大きさを s とする. b_1, b_2, $\cdots$, b_n の順序を取り替えて,

$$c_1b_1+m_2b_2+\cdots+m_nb_n\in H,\quad |c_1|=s$$

としてよい. $c_1 < 0$ のときは逆元と取り替えて $c_1 > 0$ としてよい. このとき $m_2, \cdots, m_n$ は全て c_1 で割り切れる. 仮にそうでないとすると, $m_i = q_i c_1 + r_i$, $0 \leqq r_i < c_1$, $(i = 2, \cdots, n)$ とするとき, $r_2, \cdots, r_n$ の中の少なくとも一つは 0 でない. $u_1 = b_1 + q_2 b_2 + \cdots + q_n b_n$ と置くと,

$$c_1 u_1 + r_2 b_2 + \cdots + r_n b_n = c_1 b_1 + m_2 b_2 + \cdots + m_n b_n \in H$$

となる. $u_1, b_2, \cdots, b_n$ は G の基底であり, その大きさは s よりも小さい. これは s の最小性に反する. 故に $r_i = 0$ $(2 \leqq i \leqq n)$ で $c_1 u_1 \in H$ である.

$b_2, \cdots, b_n$ で生成される G の部分群を G_0 とする. $H_0 = H \cap G_0$ は G_0 の部分群である. 任意の $h \in H$ は

$$h = q(c_1 u_1) + h_0, \quad h_0 \in H_0$$

の形に表せる. なぜなら $h = m_1 u_1 + m_2 b_2 + \cdots + m_n b_n$ を H の任意の元とするとき, $m_1 = q c_1 + r$, $0 \leqq r < c_1 = s$ とすると,

$$h - q(c_1 u_1) = r u_1 + m_2 b_2 + \cdots + m_n b_n \in H$$

となるから, s の最小性により $r = 0$ でなければならない. よって, $h_0 = m_2 b_2 + \cdots + m_n b_n \in H_0$ であって, $h = q(c_1 u_1) + h_0$ である. 帰納法の仮定により, $H_0 \neq \{0_{G_0}\}$ であれば G_0 の基底 $u_2, \cdots, u_t$ を適当に選んで, $c_2 u_2, \cdots, c_t u_t$ が H_0 の基底であって, $c_2, \cdots, c_t$ は正の整数で c_i は c_{i+1} の約数であるように出来る. 従って $u_1, u_2, \cdots, u_n$ は G の基底で, $c_1 u_1, c_2 u_2, \cdots, c_t u_t$ は H の基底である. なお, c_2 は c_1 で割り切れる. 何故ならば, $c_1 u_1 + c_2 u_2 \in H$ であるから, c_2 が c_1 で割り切れなければ, 前と同様にして $s = c_1$ の最小性に反することが示される. □

有限生成アーベル群の基本定理 13.6. 有限生成アーベル群 G は巡回群の直積に同型である[34]. 即ち, G は $G_1 \times \cdots \times G_t \times G_{t+1} \times \cdots \times G_n$ と同型である. ここで, G_i $(1 \leqq i \leqq t)$ は位数 e_i の有限巡回群で, G_i $(t+1 \leqq i \leqq n)$ は無限巡回群である. ここで $e_1 > 1$ で, e_i は e_{i+1} の約数である[35]. また, このような直積への分解は一意的に定まる.

証明. 一意性の証明は省略する. G の生成元を $a_1, a_2, \cdots, a_N$ とする. N 個の $\boldsymbol{Z}$ の直積 $H = \boldsymbol{Z} \times \boldsymbol{Z} \times \cdots \times \boldsymbol{Z}$ から G への準同型写像 f を

$$f(m_1, m_2, \cdots, m_N) = m_1 a_1 + m_2 a_2 + \cdots + m_N a_N$$

で定める. f の核 $K = \operatorname{Ker} f$ は H の部分群である. $K = \{0_H\}$ ならば, 補題 10.9 により f は単射であるから G は無限巡回群 N 個の直積 H に同型である. $K \neq \{0_H\}$ とする. 定理 13.5 によって, K は階数 T $(1 \leqq T \leqq N)$ の自由アーベル群であり, H の適当な基底 $u_1, u_2, \cdots, u_N$ が存在し

[34] 直積については §16 で詳しく述べる
[35] この条件を付けないと後の一意性は成り立たない. 問 13.1 参照.

て, $c_1u_1, c_2u_2, \cdots, c_Tu_T$ が K の基底になる. ここで, c_i は c_{i+1} の約数である. 系 12.2 より G は H/K と同型である. $H_i = \{mu_i \mid m \in \boldsymbol{Z}\}$ $(1 \leqq i \leqq N)$ と置く. $g : H \to H/K$ を自然な準同型写像とする. g を $H_i \subset H$ に制限した写像 $g_{|H_i}$ の核は $1 \leqq i \leqq T$ のときは $H_i \cap K = \{mc_iu_i \mid m \in \boldsymbol{Z}\}$ で, $T+1 \leqq i \leqq N$ のときは $\{0_H\}$ である. 従って, $G'_i = g(H_i)$ と置くと G'_i は $1 \leqq i \leqq T$ のときは位数 c_i の巡回群で, $T+1 \leqq i \leqq N$ のときは無限巡回群である. H/K が $G'_1 \times G'_2 \times \cdots \times G'_N$ に同型であることは理解し易いであろう (詳しくは §16 参照). c_i の内の最初の r 個は 1 であるとする. $t = T - r$, $n = N - r$ と置き, $e_i = c_{r+i}$ $(1 \leqq i \leqq t)$ と置く. 最初の r 個の G'_i は $\{0_G\}$ であるから, 上の直積から除いても変化はない. 故に H/K は $G'_{r+1} \times G'_2 \times \cdots \times G'_N$ の直積に同型である. 従って $G_i = G'_{i+r}$ と置くと H/K, 従って G は $G_1 \times G_2 \times \cdots \times G_n$ に同型である □

問 13.1 m, n を自然数とする. $(m, n) = 1$ のとき, C_{mn} は $C_m \times C_n$ に同型であることを示せ. ($C_m = \langle a \rangle$, $C_n = \langle b \rangle$ とする. $(a, b) \in C_m \times C_n$ は位数 mn であることを示せ.)

問 13.2 $\boldsymbol{Q}$ (演算は加法) は有限生成ではないことを示せ.

問 13.3 $\boldsymbol{Q}^* = \boldsymbol{Q} - \{0\}$ (演算は乗法) は有限生成ではないことを示せ.

問 13.4 G が $a_1, a_2, \cdots, a_n$ を基底とする自由アーベル群とする. $2G = \{2g \mid g \in G\}$ と置く. このとき指数 $[G : 2G]$ は 2^n に等しいことを示し, これによって G の全ての基底は n 個の元からなることを証明せよ.

問 13.5 有限アーベル群は位数が素数のベキである巡回群の直積に同型であることを示せ.

問 13.6 有限アーベル群 G が巡回群でなければ, ある素数 p があって G は $px = 0$ である元 x を p^2 個以上含むことを示せ.

§14* 可解群 (solvable group)

G は群とする. G 内にその部分群の列 $\{G_i\}_{0 \leqq i \leqq n}$ (n は自然数) で次の 3 条件 a), b), c) を満たすものが含まれているとき G は**可解である** (solvable) という.

a) $G_0 = G$.

b) $G_n = \{e\}$.

c) 全ての i $(0 \leqq i \leqq n-1)$ について G_{i+1} は G_i の正規部分群であって, しかも剰余類群 G_i/G_{i+1} はアーベル群である.

定義により全てのアーベル群は可解である.

本節の目標は p-群は可解であることと, 5 次以上の対称群は可解でないことを示すことにある. 以下 G は群とする.

補題 14.1.

1) G が可解であれば G の部分群は全て可解であり, G の準同型像も全て可解である.

2) G 内に正規部分群 N で, N と G/N が共に可解であるものが含まれていれば, G 自身が可解である.

証明. 1) G の部分群の列 $\{G_i\}_{0\leqq i\leqq n}$ (n は自然数) で条件 a), b), c) を満たすものをとる. さて H を G の部分群とし $H_i = H \cap G_i$ とすれば, $\{H_i\}_{0\leqq i\leqq n}$ は H に対して上の 3 条件 a), b), c) を満たす. また $f : G \to G'$ を上への準同型写像とし, $G'_i = f(G_i)$ と置くと G' の部分群の列 $\{G'_i\}_{0\leqq i\leqq n}$ は G' に対して上記の 3 条件を満たすことが確かめられる (第 12 節, 同型定理参照).
2) $G' = G/N$ と置き $f : G \to G'$ を自然な準同型写像とする. まず G' の部分群の列 $\{G'_i\}_{0\leqq i\leqq n}$ で G' に対して上記の 3 条件を満たすものをとり, $G_i = f^{-1}(G'_i)$ と置く. すると G の部分群の列 $\{G_i\}_{0\leqq i\leqq n}$ は上記の条件 a), c) 及び b') $G_n = N$ を満たす. 一方 N も可解であるから, N の部分群の列 $\{N_i\}_{0\leqq i\leqq m}$ で N に対して上記の 3 条件を満たすものがとれる. G の部分群の列 $G = G_0$, $G_1, \cdots, G_{n-1}, G_n = N, N_1, \cdots, N_m = \{e\}$ によって G も可解となる. □

G の元 a に対して $Z(a) = \{x \in G \mid ax = xa\}$ と置く. 更に $Z(G) = \{x \in G \mid G$ の全ての元 a に対して $ax = xa$ が成り立つ $\}$ と置き ***G* の中心** (the center of G) と呼ぶ. $Z(G)$ は $Z(a)$ $(a \in G)$ 全ての共通部分である. $Z(a)$ は G の部分群であり, $Z(G)$ の方は G の正規部分群でアーベル群である.

$X = G$ とする. 写像 $m_1 : G \times X \to G$ を $m_1(t, a) = tat^{-1}$ で定義する. m_1 は群の作用である (問 9.1). G 上の関係 $\sim$ を

$$\sim = \{(a, b) \in G \times G \mid \text{ 等式 } a = m_1(t, b) = tbt^{-1} \text{ が成り立つ様な } G \text{ の元 } t \text{ が存在する } \}$$

によって定める. $\sim$ は G 上の同値関係 (定義と補題 9.4) であって $a \in G$ に対し a を含む同値類 $\mathrm{C}(a)$ は $\mathrm{C}(a) = \{tat^{-1} \mid t \in G\}$ と表される. 命題 9.6 より次が従う.

補題 14.2. $|\mathrm{C}(a)| = [G : Z(a)]$.

系 14.3. 次の条件は互いに同値である.

1) $a \in Z(G)$.

2) $\mathrm{C}(a) = \{a\}$.

3) $|\mathrm{C}(a)| = 1$.

証明. 同値類 $\mathrm{C}(a)$ は a を含むから 2) と 3) は自明に同値である. $a \in Z(G)$ であることと $Z(a) = G$ は同値であって, 後者は補題 14.2 より $|\mathrm{C}(a)| = 1$ と同値である. □

$a \in Z(G)$ であるとき, この 2) は同値関係 $\sim$ については a はそれ自身で一つの類をなすことを示している. よって G が有限群であれば, この 2) より商集合 $G/\sim$ の完全代表系 $a_1, a_2, \cdots, a_m$,

$a_{m+1}, \cdots, a_r$ を $r = |G/\sim|$, $m = |Z(G)|$, $Z(G) = \{a_1, a_2, \cdots, a_m\}$ ととれることが分かる. 従って $|G| = n$ とすれば次の等式が得られる.

補題 14.4.

1) $\quad n = m + \sum_{m+1 \leqq i \leqq r} [G : Z(a_i)]$.

2) $\quad [G : Z(a_i)] \geqq 2 \ (m+1 \leqq i \leqq r)$.

さて p は素数とする. 有限群 G はその位数が p のベキであるとき p-群であるという.

補題 14.5. $\quad G$ は p-群でその位数が $n = p^s \ (s > 0)$ であれば $Z(G) \neq \{e\}$ である.

証明. $\quad Z(G) = \{e\}$ であるとしてみよう. すると $m = 1$ であるから, 補題 14.4 より等式

$$n = 1 + \sum_{2 \leqq i \leqq r} [G : Z(a_i)]$$

を得る. $p \mid n$ であるから p は $[G : Z(a_i)] \ (2 \leqq i \leqq r)$ のどれかを割り切らない. しかし定理 8.5 により $n = |Z(a_i)| \cdot [G : Z(a_i)]$ であって $n = p^s \ (s > 0)$ であるから, $[G : Z(a_i)]$ が p で割り切れないなら $[G : Z(a_i)] = 1$ である. 従ってこのような $i \ (2 \leqq i \leqq r)$ については $a_i \in Z(G)$ となるが, これは完全代表系 $a_1, a_2, \cdots, a_m, a_{m+1}, \cdots, a_r$ の取り方に反する. □

定理 14.6. $\quad p$-群は可解である.

証明. $\quad G$ は p-群で位数は $n = p^s \ (s > 0)$ であるとする. s に関する帰納法で証明する. G がアーベル群のときは主張は明らかであるから, G はアーベル群でないとする. すると $N = Z(G)$ は G の真の部分群であるから, $|N| = p^t$ であって $t < s$ である. 補題 14.5 より $|N| > 1$ であるから $t \geqq 1$ である. 故に $|G/N| = |G|/|N| = p^{s-t} < p^s$ である. 帰納法の仮定より G/N は可解であり, また N はアーベル群であるから可解である. よって補題 14.1 の 2) より G も可解である. □

補題 14.7. $\quad n \geqq 5$ とし G は S_n の部分群とする. N は S_n の正規部分群で G/N はアーベル群であると仮定せよ. このとき G が長さ 3 の巡回置換を全て含むならば, N も長さ 3 の巡回置換を全て含む.

証明. $\quad f : G \to G/N$ を自然な準同型写像とする. 文字 $1 \leqq a < b < c \leqq n$ を任意にとり, 更に a, b, c でない文字 d, $g \ (d \neq g)$ を 1 から n の範囲にとって巡回置換 $s = (d\, b\, c)$ と $t = (a\, c\, g)$ とを考えよ. G/N はアーベル群であるから $f(t)^{-1} f(s)^{-1} f(t) f(s) = e$ である. 従って $(a\, b\, c) = t^{-1} s^{-1} t s$ は f の核である N に含まれる. □

次の定理は 5 次以上の代数方程式には根の公式が存在しないという, アーベルの定理と密接に関係している.

定理 14.8. n が 5 以上であれば S_n は可解ではない.

証明. n が 5 以上でしかも S_n が可解であったと仮定しよう. $G = S_n$ と置き G の部分群の列 $\{G_i\}$ を前の 3 条件 a), b), c) を満たすようにとる. すると補題 14.7 を用いると順番に $G = G_0$, $G_1, \cdots, G_n$ は長さ 3 の巡回置換を全て含むことになるが, $G_n = \{e\}$ であるからこれは不可能である. □

問 14.1 $n \leqq 4$ のときは S_n は可解であることを確かめよ.

§15* Sylow の定理

G は有限群とし $n = |G|$ と置く. p は素数とする.

補題 15.1. $n \geqq 2$ で G とは異なる G の全ての部分群 H に対して $p \mid [G : H]$ であれば $p \mid |Z(G)|$ である.

証明. $p \mid n$ である ($H = \{e\}$ を考えよ). 補題 14.4 の 2) において $m + 1 \leqq i \leqq r$ なら $[G : Z(a_i)] \geqq 2$ より $H = Z(a_i)$ は G でない. 従って仮定により p は $[G : Z(a_i)]$ のどれも割り切る. 故に, 補題 14.4 の 1) において $p \mid m = |Z(G)|$ である. □

補題 15.2. G がアーベル群で $p \mid n$ であれば, G 内には位数が p の元 a が少なくとも一つは含まれている.

証明. 定理 13.6 より, G は巡回群の積 $G_1 \times G_2 \times \cdots \times G_t$ と同型である. 但し, G_i の位数を e_i とすると e_i は e_{i+1} の約数である. 従って e_t は p で割り切れる. $e_t = pm$ として $G_t = \langle a \rangle$ とする. このとき a^m の位数は p である. □

定理 15.3. $p^s \mid n$ であれば位数 p^s の部分群 P が少なくとも一つは G 内に含まれている.

証明. $n = 1$ であれば定理の主張は自明である. $n \geqq 2$ とし位数が $n - 1$ 以下の群については定理は正しいと仮定する. 次の二つの場合に分けて考える.

a) G 内には G ではない部分群 H で p が $[G : H]$ を割り切らないものが少なくとも一つは含まれている.

b) G とは異なる G の全ての部分群 H に対して $p \mid [G : H]$ である.

a) のときは p^s は $|H|$ を割り切り, 一方 $n > |H|$ であるから帰納法の仮定によって群 H 内に求める位数 P の部分群が存在する.

b) のときを考えると補題 15.1 より $p \mid |Z(G)|$ であるから, 補題 15.2 よりアーベル群 $Z(G)$ 内には位数が p の元 a が含まれる. $N = \langle a \rangle$ と置くと N は G の正規部分群であって $|N| = p$ であるから, $|G/N| = n/p$ は p^{s-1} で割り切れ, 帰納法の仮定より群 G/N 内には位数 p^{s-1} の部分群 P' が

含まれる. $f : G \to G/N$ を自然な準同型写像として, $f^{-1}(P') = P$ とすればこの P が求めるものである. □

以下 $n = p^s m$ と仮定する. 但し s は整数で $s \geqq 0$ であり m は自然数で $(p, m) = 1$ とする. 定理 15.3 によると G 内には位数が p^s の部分群 P が少なくとも一つは含まれている. 群 G の部分群で位数が p^s のものを G の **p-Sylow 部分群** (a p-Sylow subgroup of G) と呼ぶ. このとき次の定理が成り立つ.

Sylow の第一・第二定理 15.4.

1) P, Q がどちらも G の p-Sylow 部分群であれば, G の適当な元 a を用いて $Q = aPa^{-1}$ と表すことが出来る.

2) U が G の部分群で p-群であれば, U は G のある p-Sylow 部分群 P に含まれる.

証明. P は G の p-Sylow 部分群として, U を G の部分群でその位数が p^r のものとする. このとき G 上に関係 $\sim$ を

$$\sim = \{(a, b) \in G \times G \mid a = xby \text{ を満たす } x \in P,\ y \in U \text{ が存在する } \}$$

によって定義すると, $\sim$ は G 上の同値関係になる. G の元 a について a を含む同値類は $\mathrm{C}(a) = \{xay \mid x \in P,\ y \in U\}$ であるから, $\mathrm{C}(a)$ は集合 Pay $(y \in U)$ によって覆われている. G 上の同値関係 $\mathrm{R}_2 = \{(a, b) \in G \times G \mid ab^{-1} \in P\}$ による商集合 $X = G/\mathrm{R}_2$ は P による右剰余類の全体 $\{Pa_1, Pa_2, \cdots, Pa_k\}$ であった. 但し a_1, a_2, $\cdots$, a_k は R_2 に関する完全代表系である. U は $m_P : U \times X \to X$, $m_P(y, Pa) = Pay^{-1}$ によって G/R_2 に作用する. Pa における等方群 $N(Pa) = \{y \in U \mid Pay^{-1} = Pa\}$ は $H = U \cap a^{-1}Pa$ に等しい. 何故ならば $Pay^{-1} = Pa$ は $y \in (Pa)^{-1}Pa = a^{-1}P^{-1}Pa = a^{-1}Pa$ と同値だからである. 従って命題 9.6 より次を得る.

補題 15.5. $|\{Pay^{-1} \mid y \in U\}| = [U : H]$ である.

但し左辺は Pay^{-1} と表される相異なる右剰余類の個数である. これより直ちに次が得られる.

系 15.6. $|\mathrm{C}(a)| = |P| \cdot [U : H]$ である.

定理 15.4 の証明に戻ろう. さて商集合 $G/\sim$ の完全代表系を a_1, a_2, $\cdots$, a_t とする. $H_i = U \cap a_i^{-1}Pa_i$ $(1 \leqq i \leqq t)$ とする. すると $|H_i|$ は p のベキであるから $|H_i| = p^{r_i}$ $(r_i \leqq r)$ と書いておくと, 系 15.6 より等式

$$n = \sum_{1 \leqq i \leqq t} |\mathrm{C}(a_i)| = \sum_{1 \leqq i \leqq t} |P| \cdot [U : H_i] = p^s \cdot \sum_{1 \leqq i \leqq t} p^{r - r_i}$$

が得られる. $n = p^s m$ であるから $m = \sum_{1 \leqq i \leqq t} p^{r - r_i}$ であるが, p は m を割らないので, ある i $(1 \leqq i \leqq t)$ について $r_i = r$ でなければならない. 即ち $U = H_i$ $(= U \cap a_i^{-1}Pa_i)$ であって, U は

$a_i^{-1}Pa_i$ に含まれる. $a_i^{-1}Pa_i$ は勿論 G の p-Sylow 部分群であるから 2) は証明された. もし U も G の p-Sylow 部分群であれば, 位数を比べて $U = a_i^{-1}Pa_i$ が得られる. よって 1) も証明された.

□

系 15.7. P は G の部分群とする. G の p-Sylow 部分群が P のみであるための必要十分条件は, P が G の正規部分群であることである.

証明. P は G の正規部分群であると仮定する. Q を G の p-Sylow 部分群とすれば, 定理 15.4 の 1) より $Q = aPa^{-1}$ となる元 a を G 内にとれる. P は正規部分群であるから $aPa^{-1} = P$ であり, 従って $Q = P$ が得られる. G の任意の元 a について aPa^{-1} は G の p-Sylow 部分群であるから, もし逆に G の p-Sylow 部分群が P のみであるならば, $P = aPa^{-1}$ が G の任意の元 a について成り立ち, 確かに P は G の正規部分群である. □

Sylow の第三定理 15.8. G の p-Sylow 部分群の個数を t とすれば, t は p を法として 1 と合同であり, しかも t は n を割り切る.

この定理を証明するにはもう少し準備が必要である. 群 G の部分群 H に対して $N(H)$ を $\{a \in G \mid aH = Ha\}$ で定めると, $N(H)$ は G の部分群であって, しかも H は $N(H)$ の正規部分群となる. 更に

補題 15.9. $|\{aHa^{-1} \mid a \in G\}| = [G : N(H)]$ である.

証明. G の部分群の全体を X と置く. G は $m : G \times X \to X$, $m(a, H) = aHa^{-1}$ によって X に作用する. $N(H)$ はこの作用の H における等方群であるから, 命題 9.6 に従う. □

定理 15.8 の証明 F を G の p-Sylow 部分群の全体とする. すると定理 13.4 の 1) より $F = \{aPa^{-1} \mid a \in G\}$ であるから, 補題 15.9 より $t = [G : N(P)]$ であり従って t は n の約数である. F 上に関係 $\sim$ を

$$\sim = \{(Q, Q') \in F \times F \mid Q = aQ'a^{-1} \text{ である } a \in P \text{ が存在する }\}$$

によって定める. $\sim$ は F 上の同値関係である. $P = Q_1, Q_2, \cdots, Q_r$ を商集合 $F/\sim$ の完全代表系として $|\mathrm{C}(Q_i)| = t_i$ と置く. $\mathrm{C}(P) = \{P\}$ であるから勿論 $t_1 = 1$ である. $N_i = P \cap N(Q_i)$ と置くと, $\mathrm{C}(Q_i) = \{aQ_ia^{-1} \mid a \in P\}$ であるから, 補題 15.9 と全く同様にして $t_i = |\mathrm{C}(Q_i)| = [P : N_i]$ が得られる. さてもし $t_i = 1$ であれば, $P = N_i$ $(= P \cap N(Q_i))$ より P は $N(Q_i)$ に含まれる. すると P は $N(Q_i)$ の p-Sylow 部分群であり, Q_i も $N(Q_i)$ の p-Sylow 部分群であってしかも正規部分群であるから, 系 15.7 より $P = Q_i$ である. よって $i \neq 1$ ならば $t_i \geqq 2$ である. 一方 $t_i = [P : N_i]$ より t_i は 2 以上ならば p の倍数である. 故に $t = 1 + \sum_{2 \leqq i \leqq r} t_i$ より, t は p を法として 1 と合同である. □

§16 直積への分解

$G_1, G_2, \cdots, G_n$ が群であれば, 直積集合 $G_1 \times G_2 \times \cdots \times G_n$[36] は演算

$$(a_1, a_2, \cdots, a_n) \circ (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

によって群となる. 勿論 $G_1 \times G_2 \times \cdots \times G_n$ の単位元は $e = (e_1, e_2, \cdots, e_n)$ (e_i は G_i の単位元) であって, $(a_1, a_2, \cdots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$ である. 各 i $(1 \leqq i \leqq n)$ について写像

$$f_i : G_i \to G_1 \times G_2 \times \cdots \times G_n, \quad f_i(x) = (e_1, \cdots, e_{i-1}, x, e_{i+1}, \cdots, e_n)$$

と写像

$$p_i : G_1 \times G_2 \times \cdots \times G_n \to G_i, \quad p_i(a_1, a_2, \cdots, a_n) = a_i$$

とはどちらも準同型写像であって $p_i \circ f_i = 1_{G_i}$ となる.

次に G は群として, $G_1, G_2, \cdots, G_n$ は全て G の部分群であると仮定せよ. 各 G_i は G での積を演算にして独立した群となるから, 上に述べたようにして集合 $G_1 \times G_2 \times \cdots \times G_n$ も群になる. 更に写像

$$f : G_1 \times G_2 \times \cdots \times G_n \to G, \quad f(a_1, a_2, \cdots, a_n) = a_1 a_2 \cdots a_n$$

を考えることが出来る. 但しこの写像 f は必ずしも準同型写像ではない.

補題 16.1. f が準同型写像であるための必要かつ十分な条件は, $x \in G_i$, $y \in G_j$ $(i \neq j)$ ならば, 常に $xy = yx$ が成り立つことである.

証明. $f_i(x) f_j(y) = f_j(y) f_i(x)$, $f(f_i(x)) = x$, $f(f_j(y)) = y$ であるから, もし f が準同型写像であれば,

$$xy = f(f_i(x)) f(f_j(y)) = f(f_i(x) f_j(y)) = f(f_j(y) f_i(x)) = f(f_j(y)) f(f_i(x)) = yx$$

を得る. 逆に $x \in G_i$, $y \in G_j$ $(i \neq j)$ ならば $xy = yx$ であると仮定せよ. すると順番に入れ替えて, $a_i, b_i \in G_i$ $(1 \leqq i \leqq n)$ について $(a_1 b_1)(a_2 b_2) \cdots (a_n b_n) = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)$ が成り立つことを容易に示せる. 従って f は準同型写像である. □

定理 16.2. f が同型写像であるためには, 次の 3 条件が満たされることが必要かつ十分である.

1) $G = G_1 G_2 \cdots G_n$.

2) G_i $(1 \leqq i \leqq n)$ は全て G の正規部分群である.

3) 全ての i $(1 \leqq i \leqq n)$ について, G_i と $G_1 \cdots G_{i-1} G_{i+1} \cdots G_n$ の共通部分は単位元のみである.

このとき, f は単射であるから G の元 g を $g = a_1 a_2 \cdots a_n$ $(a_i \in G_i)$ の形に表す表し方は唯一通りである. また, 群 G は部分群 $G_1, G_2, \cdots, G_n$ の直積[37] に分解されると言う.

---

[36] ここで $G_1, G_2, \cdots, G_n$ は相互に関連のない群である. この様な直積を外部直積という.

[37] ここで $G_1, G_2, \cdots, G_n$ は G の部分群であるから相互に関連している. この様な直積を内部直積という.

証明. 1), 2), 3) が満たされていると仮定せよ. $x \in G_i$, $y \in G_j$ $(i \neq j)$ とする. このとき 2) より, $z = xyx^{-1}y^{-1}$ は $z = (xyx^{-1})y^{-1}$ と見ることによって $z \in G_j$ であり, $z = x(yx^{-1}y^{-1})$ と見ることによって $z \in G_i$ となる. $z \in G_i$ かつ $z \in G_j$ であるから, 3) より $z = e$ であり $xy = yx$ を得る. よって補題 16.1 より f は準同型写像である. 1) より無論 f は全射である. $\mathrm{Ker}\, f$ の元 $(a_1, a_2, \cdots, a_n)$ を取ろう. すると $a_1a_2\cdots a_n = e$ であるが, 上に示したように $a_ia_j = a_ja_i$ なので, $a_i^{-1} = a_1\cdots a_{i-1}a_{i+1}\cdots a_n$ であり, 従って 3) より $a_i^{-1} = e$ 即ち $a_i = e$ を得る. よって $(a_1, a_2, \cdots, a_n) = (e, e, \cdots, e)$ であって f は単射となる.

逆に f は同型であると仮定しよう. f は全射であるから 1) が得られる. $x \in G_i$ とし $a \in G$ とせよ. f は全射であるから $a = a_1a_2\cdots a_n$ $(a_i \in G_i)$ と表される. しかも補題 16.1 より $j \neq i$ であれば任意の $y \in G_j$ について $xy = yx$ であるから,

$$axa^{-1} = a_1a_2\cdots a_nxa_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1} = a_1a_2\cdots a_{i-1}(a_ixa_i^{-1})a_{i-1}^{-1}\cdots a_1^{-1}$$

である. ここで $a_ixa_i^{-1}$ は G_i の元であるから更に入れ替えることが出来て, 結局 $axa = a_ixa_i^{-1}$ となり $axa^{-1} \in G_i$ であることが分かり 2) を得る. x を G_i と $G_1\cdots G_{i-1}G_{i+1}\cdots G_n$ の共通部分の元とする. すると $x = a_1\cdots a_{i-1}a_{i+1}\cdots a_n$ $(a_i \in G_i)$ と表すと, x^{-1} は G_i の元だから $a_jx^{-1} = x^{-1}a_j$ であって, 従って $a_1\cdots a_{i-1}x^{-1}a_{i+1}\cdots a_n = e$ となる. よって $(a_1, \cdots, a_{i-1}, x^{-1}, a_{i+1}, \cdots, a_n)$ は $\mathrm{Ker}\, f$ の元であって, f は単射であるから $x^{-1} = e$ となって $x = e$ が得られる. □

系 16.3. G は群で H, K は G の部分群とする. このとき G が H と K の直積に分解されるための必要かつ十分な条件は, 1) $G = HK$, 2) H も K も G の正規部分群であってかつ, 3) H と K の共通部分は単位元だけから成ることである.

定理 13.6 の証明の続き 定理 13.6 の中の H/K が G_1', G_2', $\cdots$, G_N' の直積に同型であることを示す. H/K の任意の元は $g(m_1u_1+m_2u_2+\cdots+m_Nu_N)$ と表せる. これは $g(m_1u_1)+g(m_2u_2)+\cdots+g(m_Nu_N)$ に等しい. $g(m_iu_i)$ $(1 \leqq i \leqq N)$ は $G_i' = g(H_i)$ の元であるから 1) は正しい. アーベル群の部分群は常に正規部分群である (問 10.2) から 2) も正しい. G_i' と $G_1'\times\cdots G_{i-1}'\times G_{i+1}'\times\cdots\times G_N'$ の共通部分に含まれる元 a をとる.

$$a = g(m_iu_i) = g(m_1u_1) + \cdots + g(m_{i-1}u_{i-1}) + g(m_{i+1}u_{i+1}) + \cdots + g(m_Nu_N)$$

と表せる. 従って

$$g(m_1u_1 + \cdots + m_{i-1}u_{i-1} - m_iu_i + m_{i+1}u_{i+1} + \cdots + m_Nu_N) = 0_{H/K}$$

である. よって

$$m_1u_1 + \cdots + m_{i-1}u_{i-1} - m_iu_i + m_{i+1}u_{i+1} + \cdots + m_Nu_N \in K$$

を得る. 故に $c_i \mid m_i$ $(1 \leqq i \leqq T)$ 及び $m_i = 0$ $(T+1 \leqq i \leqq N)$ を得る. 従って, 全ての i に対して $g(m_iu_i) = 0_{H/K}$ であり, よって $a = 0_{H/K}$ である. 即ち 3) も正しい. □

このノートを閉じる前に Sylow の定理のささやかな応用を述べてみたい. 以下 G は有限群とする.

補題 16.4. H, K を G の部分群とし, J を H と K の共通部分とする. このとき,

1) 等式 $|HK| = |KH| = |H| \cdot |K|/|J|$ が成り立つ.

2) $(\,|H|, |K|\,) = 1$ であれば, $|HK| = |KH| = |H| \cdot |K|$ である.

証明. 1) K 上の同値関係 R_1 を

$$R_1 = \{(k, k') \in K \times K \mid k^{-1}k' \in J\}$$

で定める. 集合 K から集合 $X = \{kH \mid k \in K\}$ への写像 $g : K \to X$, $g(k) = kH$ は全射であってかつ $R_g = R_1$ を満たす. よって系 2.7 より $[K : J] = |K/\mathrm{R}_1| = |X|$ である. 集合 KH は集合 kH $(k \in K)$ で覆われるから, $|KH| = [K : J] \cdot |H|$ が成り立つ. よって $|KH| = (\,|K|/|J|\,) \cdot |H| = (\,|K| \cdot |H|\,)/|J|$ である. H, K の対称性より $|HK| = (\,|K| \cdot |H|\,)/|J|$ でもある.

2) $|J| \mid |K|$ かつ $|J| \mid |H|$ であるから $|J| = 1$ となる. □

例題 16.5. $|G| = 6$ であれば, G は $C_6 = C_2 \times C_3$ か又は S_3 に同型である.

証明. H を G の 3-Sylow 部分群, K を G の 2-Sylow 部分群とすると, 補題 16.4 の 2) より $|HK| = 6$ である. よって $G = HK$ となる. $H = \langle a \rangle$, $K = \langle b \rangle$ と置く. もし $ab = ba$ ならば, $o(ab) = n$ と置くと, $(ab)^n = a^n b^n = e$ より $a^n = b^{-n}$ は H と K の共通部分 J に含まれる. $J = \{e\}$ であるから, $a^n = b^{-n} = e$ となって, $3 \mid n$ かつ $2 \mid n$ を得る. よって $6 \mid n$ である. $n \mid 6$ より $n = 6$ で, この場合は G は C_6 と同型である. $ab \neq ba$ とせよ. すると $H = \{e, a, a^2\}$, $K = \{e, b\}$ である. $G = HK$ より $G = \{e, a, a^2, b, ab, a^2b\}$ であるが, ba の可能性は $ba = a^2b$ しかない. これを手掛かりに G の乗積表を作ると, S_3 のそれに一致していることが確かめられる. □

補題 16.6. $|G| = p^2$ (p は素数) であれば, G はアーベル群である.

証明. 補題 14.5 より $Z = Z(G)$ の位数は p 又は p^2 である. G がアーベル群でないとすれば $|Z| = p$ である. $a \in G$ を Z に含まれないように取り $H = \langle a \rangle$ と置く. G はアーベル群でないので a の位数は p である (a の位数が p^2 であると G は位数 p^2 の巡回群になってアーベル群になる). すると H と Z は $|H| = |Z| = p$ で $H \neq Z$ であるから $H \cap Z$ は Z の真の部分群である. よって $H \cap Z$ の位数は 1 であるから $H \cap Z = \{e\}$ であり, 補題 16.4 の 1) より $G = HZ$ である. ここで H はアーベル群だから G もアーベル群になる (確かめよ). これは矛盾である. □

系 16.7. $|G| = p^2$ (p は素数) であれば, G は C_{p^2} か又は $C_p \times C_p$ と同型である.

証明. 補題 16.6 と定理 13.6 による. □