代数学概論 A 演習

黒木 玄　(東北大学理学研究科)

2014 年 10 月 7 日 (火)

目 次

1 商集合

1.1 同値関係, 集合の分割, 全射の関係

この節では, 同値関係, 集合の分割, 全射の関係を解説する. それらの総体が商集合の概念を構成するのである.

定義 1.1 (同値関係) 集合 A における関係 $\sim$ が**同値関係 (equivalence relation)** であるとは, $\sim$ が A の要素に関して以下を満たしていることである:

反射律 $x \sim x$,

対象律 $x \sim y \implies y \sim x$,

推移律 $x \sim y$ and $y \sim z \implies x \sim z$. □

定義 1.2 (分割) 集合 A の部分集合の集合 $\mathcal{Q}$ が以下の条件を満たしているとき, $\mathcal{Q}$ は A の**分割 (類別, partition)** であると言う:

- $A = \bigcup_{X \in \mathcal{Q}} X$,
- $\forall X \in \mathcal{Q},\ X \neq \emptyset$,
- $\forall X, Y \in \mathcal{Q},\ X \neq Y \implies X \cap Y = \emptyset$. □

命題 1.3 (全射) 写像 $f : A \to B$ が全射 (surjection) であることと $\forall y \in B,\ f^{-1}(y) \neq \emptyset$ が成立していることは同値である. □

同値関係から分割と全射を構成 $\sim$ は集合 A における同値関係であるとする. A の $\sim$ による商 $A/\sim$ を次のように定める:

$$A/\sim := \{\, [x] \mid x \in A \,\}, \quad (\text{ここで } [x] := \{\, y \in A \mid y \sim x \,\}).$$

このとき, $A/\sim$ は A の分割であり, 写像 $p : A \to A/\sim$ を $p(x) = [x]$ $(\forall x \in A)$ と定めると, p は全射である.

分割から同値関係と全射を構成 $\mathcal{Q}$ は集合 A の分割であるとする. このとき, A における同値関係 $\sim$ を

$$x \sim y \iff \exists X \in \mathcal{Q} \,\text{s.t.}\, x \in X \,\text{and}\, y \in X$$

と定めることができ, $A/\sim = \mathcal{Q}$ が成立する. また, 上で定義した全射 p を $\forall x \in A,\ x \in p(x) \in \mathcal{Q}$ という条件で定めることもできる.

全射から同値関係と分割を構成 全射 $f : A \to B$ に対して, A における同値関係 $\sim$ を

$$x \sim y \iff f(x) = f(y)$$

によって構成できる. このとき,

$$A/\sim = \{\, f^{-1}(y) \mid y \in B \,\}$$

が成立している. さらに, 全単射 $\phi : A/\sim \to B$ を

$$\phi([x]) := f(x) \quad \forall x \in A$$

によって定めることができる.

[1] 以上の 3 つの構成を証明付きで説明せよ. □

このように, 同値関係, 分割, 全射の概念は商集合という 1 つの概念を別のやり方で表現したものだと言って良い.

商集合の元 $[x] \in A/\sim$ に対して, 任意の $y \in [x]$ を類 $[x]$ の代表元 (representative) と呼ぶ. 部分集合 $B \subset A$ が類別 $A/\sim$ の完全代表系 (complete system of representatives) であるとは, 任意の類 $[x] \in A/\sim$ と B の共通部分が 1 点集合になることである定義する. 任意の類別の完全代表系が取れることと選択公理は同値である.

1.2 任意の関係から生成された同値関係

集合 A, B の直積の部分集合 $R \subset A \times B$ を A と B の間の関係 (relation) と呼び, $A = B$ のとき R は A における関係であると言う. $(x, y) \in R$ であることを xRy と略記することも多い.

集合 A, B, C 対して, 関係 $R \subset A \times B$, $S \subset B \times C$ に対して, 関係 $S \circ R \subset A \times C$ を

$$S \circ R := \{\, (x, z) \in A \times C \mid \exists y \in B \,\text{s.t.}\, xRy \,\text{and}\, ySz \,\}$$

と定義する. これを R と S の合成 (composition) と呼ぶ.

集合 A に対して, $=$ の定める A における関係を $\Delta_A := \{\, (x, x) \mid x \in A \,\}$ と表わす.

関係 $R \subset A \times B$ に対して, その転置 $R^t \subset B \times A$ を $R^t := \{\, (y, x) \mid (x, y) \in R\}$ と定める.

[2] 集合 A, B, C, D に対して以下が成立する:

1. 関係 $R \subset A \times B$, $S \subset B \times C$, $T \subset C \times D$ に対して, $T \circ (S \circ R) = (T \circ S) \circ R$.
2. $R \circ \Delta_A = \Delta_B \circ R = R$.
3. $(S \circ R)^t = R^t \circ S^t, \quad (\Delta_A)^t = \Delta_A$. $\square$

このように, 集合の間の関係は, 集合の間の写像と同様に, 合成に関して結合律を満たし, 単位元を持つ.

R は集合 A における任意の関係であるとする.

R の n 回の合成 $R \circ \cdots \circ R$ を一時的に R^n と略記する. $R^0 := \Delta_A$ と置く. (Δ_A は $=$ に対応する A における関係である.)

R が反射律を満たしてなくても, A における関係 S を

$$xSy \iff x = y \,\text{or}\, xRy$$

と定めると S は反射律を満たす. S は集合として R を含み反射律を満たす最小の関係である. 特に, R が反射律を満たすことと $R = S$ は同値である. 集合としては $S = \Delta_A \cup R = R^0 \cup R^1$ である.

R が対称律を満たしてなくても, A における関係 S を

$$xSy \iff xRy \,\text{or}\, yRx$$

と定めると S は対称律を満たす. S は集合として R を含み対称律を満たす最小の関係である. 特に, R が対称律を満たすことと $R = S$ は同値である. 集合としては $S = R \cup R^t$ である.

R が推移律を満たしてなくても, xSy を

> 長さ 2 以上の列 $x_0, \ldots, x_n$ で $x = x_0, x_0Rx_1, x_1Rx_2, \ldots, x_{n-1}Rx_n, x_n = y$ を満たすものが存在することである

と定義することによって A における関係 S を定めると S は推移律を満たす. S は集合として R を含み推移律を満たす最小の関係である. 特に, R が推移律を満たすことと $R = S$ は同値である. 集合としては $S = \bigcup_{n=1}^{\infty} R^n$ である.

R が同値関係でなくても, 関係 T を

$$xSy \iff xRy \text{ or } yRx;$$
$$xTy \iff \exists n \in \mathbb{N}\, \exists x_0, \ldots, x_n \text{ s.t. } x = x_0, x_0Sx_1, x_1Sx_2, \ldots, x_{n-1}Sx_n, x_n = y$$

と定めると T は同値関係になる. T は集合として R を含む最小の同値関係である. 特に, R が同値関係であることと $R = T$ は同値である. 集合としては $T = \bigcup_{n=0}^{\infty}(R \cup R^t)^n$ である[1]. この T を R から生成された同値関係と呼ぶ.

[3] 以上の結果を証明せよ. □

2 群に関する基本的な事柄

2.1 群 (group) の定義

この節では群 (group) の定義を行なう.

実際には, 群ではではなく, 環 (ring), 可換環 (commutative ring), 斜体 (skew field), 体 (field), 代数 (多元環, algebra) などなども定義しておかなければ, 極めて不便である. 群の理論は群だけでは決して閉じないのである[2]. しかし, それらの定義は講義や教科書にまかせて省略する. もちろん, それらの言葉をこの演習で自由に用いるかもしれないので, 自学自習しておくことが望ましい.

定義 2.1 (群 (group)) 集合 G, 2 項演算 $\cdot : G \times G \to G$, $(x, y) \mapsto xy$, 要素 $1 \in G$, 単項演算 $G \to G$, $x \mapsto x^{-1}$ の 4 つ組で以下の公理を満たすものを**群 (group)** と呼ぶ:

結合律 $(xy)z = x(yz) \quad (\forall x, y, z \in G)$;

単位元 $1x = x1 = x \quad (\forall x \in G)$;

逆元 $x^{-1}x = xx^{-1} = 1 \quad (\forall x \in G)$.

要素 1 を G の単位元, x^{-1} を x の逆元と呼ぶ. このとき G は群であると言う. 群 G がさらに次を満たしているとき, G を**可換群 (commutative group)** もしくは **Abel 群 (Abelian group)** と呼ぶ:

可換性 $xy = yx \quad \forall x, y \in G$.

Abel 群の $\cdot$, 1, $(\ \ )^{-1}$ をそれぞれ $+$, 0, $-(\ \ )$ と書くことがある. そのとき G は**加法群 (additive group)** であると言う. 群 G が有限集合であるとき, G は**有限群 (finite group)** であると言い, G の要素の個数を G の**位数 (order)** と呼ぶ. □

---

[1] 数もしくは作用素の類に関しては $\sum_{n=0}^{\infty} A^n$ を Neumann 級数と呼ぶ. 収束するとき, それは $(1-A)^{-1}$ に等しくなる. ここでは形式的に関係 $S = R \cup R^t$ の Neumann 級数もどきが現われていることに注意せよ.

[2] このことはあらゆる数学に当てはまる.

[4] 集合 G に結合律を満たす 2 項演算 $\cdot : G \times G \to G$ が与えられているとき以下が成立する:

(1) $1_L, 1_R \in G$ が $1_L x = x 1_R = x$ $(\forall x \in G)$ を満たしていれば $1_L = 1_R$ である. (つまり, 左単位元と右単位元は一致する.)

(2) $1_L \in G$ が $1_L x = x$ $(\forall x \in G)$ を満たしていたとしても, $x 1_R = x$ $(\forall x \in G)$ を満たす $1_R \in G$ が存在しない場合がある. (つまり, 左単位元があっても, 右単位元があるとは限らない.)

(3) $1 \in G$ が $1x = x1 = x$ $(\forall x \in G)$ を満たしているとき, 任意の $a, l, r \in G$ に対して $la = ar = 1$ ならば $l = r$ である. (つまり, 両側単位元が存在するとき, 左逆元と右逆元は一致する.)

(4) $1_L x = x$ $(\forall x \in G)$ を満たす要素 $1_L \in G$ と $x^L x = 1_L$ $(\forall x \in G)$ を満たす写像 $(\ )^L : G \to G$ が存在するならば G は群である. (つまり, 左単位元と左逆元を持つような結合律を満たす 2 項演算が与えられた集合は群である.)

(5) $1_L x = x$ $(\forall x \in G)$ を満たす要素 $1_L \in G$ と $x x^R = 1_L$ $(\forall x \in G)$ を満たす写像 $(\ )^R : G \to G$ が存在しても, G が群にならない場合がある. (つまり, 左単位元と右逆元があっても群になるとは限らない.) □

ヒント:

(2) 写像 $p : A \to A$ が $p \circ p = p$ を満たしていると仮定する. $G := \{\, p \circ f \mid f : A \to A \,\}$ と置き, G に 2 項演算を写像の合成によって定めておく. このとき, その 2 項演算は結合律を満たし, $p \in G$ は左単位元になる. しかし, $\mathrm{id}_A \notin G$ であることもあり得るので, 右単位元が存在するとは限らない. そのような例を具体的に構成して調べてみよ.

(4) $x = 1_L x = x^{LL} x^L x = x^{LL} 1_L$ なので $x x^L = x^{LL} 1_L x^L = x^{LL} x^L = 1_L$. よって, $x 1_L = x x^L x = 1_L x = x$.

(5) 集合 A と $a \in A$ に対して, $B := A - \{a\}$ と置き, G を次のように定める:

$$G = \{\, f : A \to A \mid f \text{ の } B \text{ への制限は } B \text{ から } B \text{ への全単射であり, } f(a) \in B \,\}.$$

G は写像の合成に関して閉じているので, 写像の合成によって結合律を満たす 2 項演算を G に定めることができる. そのとき, 任意の $b \in B$ に対して, $1_b \in G$ を $1_b(x) = x$ $(x \in B)$, $1_b(a) = b$ と定めると, 1_b は G の左単位元である. $f \in G$ に対して $f^R \in G$ を $f^R(x) = f^{-1}(x)$ $(x \in B)$, $f^R(a) = f^{-1}(b)$ と定めると $f \circ f^R = 1_b$ が成立する. しかし, $f(a) \neq f(b)$ を満たす $f \in G$ に対して $g \circ f = 1_b$ を満たす $g \in G$ は存在しない. このような f は B が 2 つ以上の元を持てば存在する. 以上の議論の細部を埋めよ.

[5] (群の直積) G, H が群であるとき, $G \times H$ に積を $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ $(g_i \in G, h_i \in H)$ と定義すると $G \times H$ は自然に群をなす. □

群の部分集合 $A \subset G$ が G を**生成する (generate)** もしくは G の**生成系 (generating system)** であるとは, G の任意の元を A の元およびその逆元の有限個の積で表わすことができることであると定義する. ただし 0 個の元の積は単位元になると約束しておく. 唯一の元から生成される群を**巡回群 (cyclic group)** と呼ぶ.

[**6**] 以下を示せ:

1. $\mathbb{Z}$ は加法に関して巡回群である.
2. 任意の巡回群は Abel 群である.
3. 位数が素数に等しい有限群は巡回群である. □

2.2 部分群と剰余類 (subgroup and coset)

定義 2.2 (部分群 (subgroup)) G が群であるとき, $H \subset G$ が

- $x, y \in H \implies xy \in H$,
- $1 \in H$,
- $x \in H \implies x^{-1} \in H$

を満たしていれば, G の演算を H に制限することによって, H は自然に群とみなせる. このとき, H は G の**部分群 (subgroup)** であると言う. □

群 G の部分群 H, K と $a \in G$ に対して次のように置く:

- $HK := \{\, xy \mid x \in H \,\text{and}\, y \in K \,\}, \quad H^{-1} := \{\, x^{-1} \mid x \in H \,\}.$
- $Ha := \{\, xa \mid x \in H \,\}, \quad aK := \{\, ax \mid x \in K \,\}, \quad HaK := \{\, xay \mid x \in H \,\text{and}\, y \in K \,\}.$

Ha を a の**右剰余類 (right coset)** と呼び, aH を a の**左剰余類 (left coset)** と呼び, HaK を a の**両側剰余類 (two-sided coset)** と呼ぶ.

[**7**] G が群であるとき, $H \subset G$ が部分群であるための必要十分条件は, $HH \subset H$, $1 \in H$, $H^{-1} \subset H$ が成立することである. □

さらに, 以下のように置く:

- $H\backslash G := \{\, Hx \mid x \in G \,\}$;
- $G/K := \{\, xK \mid x \in G \,\}$;
- $H\backslash G/K := \{\, HxK \mid x \in G \,\}$.

それぞれを, G を H で左から割ってできる**右剰余類空間 (right coset space)**, G を H で右から割ってできる**左剰余類空間 (left coset space)**, G を H と K で左右から割ってできる**両側剰余類空間 (two-sided coset space)** と呼ぶ.

[8] 群 G のその部分群 K に対して, G の同値関係 $\sim$ を

$$x \sim y \iff \exists h \in K \text{ s.t. } xh = y$$

によって定めることができる. 右辺の条件は $xK = yK$, $y \in xK$ のそれぞれと同値であり. このとき, $G/K = G/\sim$ が成立している. これを証明し, $H\backslash G$ と $H\backslash G/K$ についても同様の結果が成立していることを説明せよ. □

2.3 群の作用 (action of group) の定義

群 G が集合 X に左から (もしくは右から) **作用 (act)** しているとは, 以下を満たす $\cdot : G \times X \to X$ (もしくは $\cdot : X \times G \to X$) が与えられていることである:

- $(gh)x = g(hx)$ (もしくは $x(gh) = (xg)h$) $\quad \forall g, h \in G$, $\forall x \in X$;
- $1x = x$ (もしくは $x1 = x$) $\quad \forall x \in X$.

G が (左もしくは右から) 作用する集合のことを (左もしくは右) G 集合と呼ぶことにする.

[9] **(置換群と対称群)** 以下を示せ:

1. 任意の集合 X に対して, $\mathrm{Aut}\, X$ を X からそれ自身への全単射全体の集合と定め, $\mathrm{Aut}\, X$ の 2 項演算を写像の合成によって定めると, $\mathrm{Aut}\, X$ は自然に群をなす.
2. さらに, $\mathrm{Aut}\, X$ は X に左から自然に作用している.

$\mathrm{Aut}\, X$ は集合 X の置換群 (permutation group) と呼ばれている. 特に $A = \{1, 2, \ldots, n\}$ であるとき, $S_n := \mathrm{Aut}\, A$ と置き, S_n を n 次の対称群 (symmetric group) と呼ぶ. S_n の位数は $n!$ である. □

$\mathrm{Aut}\, X$ の部分群を集合 X の**変換群 (transformation group)** と呼ぶ. 群の具体例の多くが変換群として与えられる. それはなぜかと言うと, 群論はある意味で空間の対称性 (symmetry) を扱う分野だからである. これがどういう意味なのか知りたい人は, あとで群の具体例に関する問題を大量に出すので, そちらを見て欲しい. とにかく, 群論においては, 群そのものを考えるだけでは不十分であり, **群とその作用の組を考えることが重要である**ことを忘れてはならない!

参考 以下はすぐには理解できない思想に関する話なので難しいと思ったら読み飛ばして欲しい:

- 幾何的な空間とそこに作用する変換群の組によって幾何学を分類するという思想が, Felix Klein による有名なエルランゲン・プログラム (Erlanger Programm) である.
- これとは別に G. F. B. Riemann の多様体の幾何学という思想がある. 多様体は一般に対称性がほとんどないし群も作用していない.

- これらの思想はファイバー・バンドルの理論で統一されている. すなわち, 多様体の各点に Klein の意味での変換群の幾何学が乗っているような状況を呼ぶ考え, それが多様体方向に接続を通して繋がっているという状況を考えることができるのである. この考え方はゲージ理論や保型形式論など広い応用範囲を持っている.

以下, 簡単のため多くの場合において, 左作用のみに関して説明する. 右作用に関しても同様である.

左 G 集合の間の写像 $\phi : X \to Y$ が G 準同型 (写像) であるとは, $\phi(gx) = g\phi(x)$ $(x \in X)$ が成立することであると定める.

[10] G 集合の間の G 準同型の合成も準同型であり, G 集合 X に対して id_X も G 準同型である. G 準同型が全単射であるとき, その逆写像も G 準同型である. そのときその全単射 G 準同型を G 同型と呼ぶ. □

以下, 群 G が集合 X に左から作用しているとする.

$x \in X$ の G 軌道 (G-orbit) とは集合 $Gx = \{\, gx \mid g \in G \,\}$ のことである.

$x \in X$ に対して, $G_x := \{\, g \in G \mid gx = x \,\}$ と置くと, G_x は G の部分群をなす. G_x を点 x における**等方部分群 (isotropy subgroup)** もしくは点 x の**固定部分群 (subgroup of stability)** と呼ぶ.

[11] (軌道と剰余類空間の同型) 以下を示せ:

1. G の任意の部分群 H に対して, 左剰余類空間 G/H は $g(xH) := (gx)H$ $(g, x \in G)$ によって自然に左 G 集合である.

2. 左 G 集合 X と点 $x \in X$ に対して, G 同型 $\phi : G/G_x \to Gx$ を $\phi(gG_x) := gx$ $(g \in G)$ によって定めることができる.

3. G の X への作用が**推移的 (transitive)** であるとは G の軌道が唯一つで X 全体に一致してしまうことであると定義する. 上の結果より, G の X への作用が $transitive$ であれば, 点 $x \in X$ を選ぶごとに, G/G_x から X への G 同型が自然に得られる. □

X の G の作用による**商空間 (quotient space)** もしくは**軌道空間 (orbit space)** とは,

$$G\backslash X := \{\, Gx \mid x \in X \,\}$$

のことである.

[12] X における同値関係 $\sim$ を

$$x \sim y \iff \exists g \in G \,\mathrm{s.t.}\, gx = y$$

と定めることができる. この右辺の条件は $y \in Gx$, $Gx = Gy$ のそれぞれと同値である. このとき, $G\backslash X = X/\!\sim$ が成立する. この類別を X の G の作用による**軌道分解 (orbit decomposition)** と呼ぶ. □

[13] 群 G とその部分群 H を考える. H は左からの積によって G に自然に作用している. この左作用に関する軌道空間は第 2.2 節で定義された $H\backslash G$ に等しい. □

2.4 群の表現 (representation of group) の定義

V は体 K 上のベクトル空間であるとする. G の V への左作用が線形であるとき, すなわち,

$$g(v_1+v_2)=gv_1+gv_2,\quad g(kv)=k(gv)\quad (g\in G,\ v,v_i\in V,\ k\in K)$$

が成立しているとき, G の V への作用は G **の (左) 表現 ((left) representation of** G**)** と呼ばれている.

[14] (一般線形群) V は体 K 上のベクトル空間であるとする. このとき, V のベクトル空間としての同型写像全体 $GL(V)$ は写像の合成に関して自然に群をなし, $GL(V)$ の V への自然な作用は $GL(V)$ の V における表現である. $GL(V)$ は一般線形群 (general linear group) と呼ばれている. 特に $V=K^n$ のとき, $GL_n(K):=GL(V)$ と書く. $GL_n(K)$ は可逆な $n\times n$ 行列全体のなす群と同一視できる. □

V, W は体 K 上のベクトル空間であり, V, W における G の左表現が定められていると仮定する. このとき, 線形写像 $\phi: V\to W$ が G の表現の準同型 (homomorphism of representations of G) もしくはより簡潔に G 準同型 (G-homomorphism) であるとは, $\phi(gv)=g\phi(v)$ $(g\in G,\ v\in V)$ が成立していることであると定義する.

[15] G の表現の間の G 準同型の合成も準同型であり, G の表現 V に対して id_V も G 準同型である. 表現の G 準同型が全単射であるとき, その逆写像も表現の G 準同型である. そのときその全単射 G 準同型を G の表現の同型写像と呼ぶ. □

[16] (群の作用の量子化) 群 G が集合 X と Y に右から作用しているとする. さらに, X と Y は有限集合であると仮定する. 任意の集合 A に対して, 体 K に値を持つ A 上の函数の全体のなす K 上のベクトル空間を $\mathrm{Func}(A)$ と書くことにし, $V=\mathrm{Func}(X)$, $W=\mathrm{Func}(Y)$ と置く. このとき, 以下を示せ:

1. G の V における左表現を $(g\phi)(x):=\phi(xg)$ $(g\in G,\ \phi\in V,\ x\in X)$ によって定めることができる. W についても同様である.
2. V から W への線形写像 L と $X\times Y$ 上の K 値函数 $k\in\mathrm{Func}(X\times X)$ は
$$(L\phi)(y):=\sum_{x\in X}\phi(x)k(x,y)\quad (\phi\in V,\ y\in Y)$$
によって一対一に対応している. (ヒント: 数ベクトルと行列の理論.)
3. id_V に対応する $k\in\mathrm{Func}(X\times X)$ は Kronecker のデルタ $k(x,y)=\delta_{x,y}$ $(x,y\in X)$ である. ($\delta_{x,y}$ は $x=y$ なら 1 であり, そうでないなら 0 である.)
4. $k\in\mathrm{Func}(X\times Y)$ が V から W への G 準同型に対応するための必要十分条件は $k(xg,yg)=k(x,y)$ $(x,y\in X,\ g\in G)$ が成立することである.
5. 特に, G のある部分群 H, K について $X=H\backslash G$, $Y=K\backslash G$ であるならば, G 準同型を与える函数 $k\in\mathrm{Func}(X\times Y)$ と 両側剰余類空間上の函数 $f\in\mathrm{Func}(H\backslash G/K)$ が $k(Hx,Ky)=f(Hxy^{-1}K)$ $(x,y\in G)$ によって一対一に対応する.

両側剰余類空間の重要性はこのような考察をしてみるとよくわかる. □

参考 以下はすぐには理解できない思想に関する話なので難しいと思ったら読み飛ばして欲しい:

- 変換群とその作用の組を考察することはある意味で群論の古典力学版であると言える. これに対して, 群とその表現を考察することは群論の量子力学版であると言える. そして, 群の表現を幾何的に構成するためには, 群が作用する多様体の上の函数空間を考え, そこへの群の作用を考えれば良いことが知られている (古典論の量子化).
- エルランゲン・プログラムや Riemann の幾何学の量子力学版を考えることができる. ファイバー・バンドルの幾何学の量子力学版は場の量子論である.
- 実は, おおっぴらに言っている人を見たことがないが, あらゆる数学は何らかの意味で量子化されねばならないという思想が現代にはあって, 実際その思想のもとで様々な数学の様々な量子化が研究されている.

2.5 群の準同型 (homomorphism)

定義 2.3 (群の準同型 (homomorphism of groups)) 群の間の写像 $f : G \to H$ が (群の) 準同型写像 (homomorophism) であるとは, f が $f(xy) = f(x)f(y)$, $f(1) = 1$, $f(x^{-1}) = f(x)^{-1}$ $(\forall x, y \in G)$ を満たしていることである. □

[17] (群の準同型写像) 以下を示せ:

1. 群の間の写像 $f : G \to H$ が $f(xy) = f(x)f(y)$ $(\forall x, y \in G)$ のみを満たしていることと, f が準同型であることは同値である.
2. 群 G の恒等写像 id_G は準同型であり, 準同型写像の合成もまた準同型である.
3. 準同型写像が逆写像を持てばその逆写像も準同型である. 逆写像を持つような群の準同型写像を群の**同型写像 (isomorphism of groups)** と呼ぶ. □

[18] 群 G の集合 X への左作用と G から X からそれ自身への全単射全体のなす群 $\mathrm{Aut}\, X$ への準同型写像は自然に一対一に対応していることを示せ. □

ヒント: $\rho : G \to \mathrm{Aut}\, X$ と $\alpha : G \times X \to X$ の間の自然な対応 $\rho(g)(x) = \alpha(g, x)$ を考えよ.

[19] V が体 K 上のベクトル空間であるとき, 群 G の V における左表現と G から $GL(V)$ への準同型写像が自然に一対一に対応していることを示せ. □

定義 2.4 (正規部分群 (normal subgroup)) 群 G の部分群 H が G の**正規部分群 (normal subgroup)** であるとは, 任意の $g \in G$ に対して $Hg = gH$ $(i.e.,\ gHg^{-1} = H)$ が成立することである. G が G 自身と $\{1\}$ 以外の正規部分群を持たないとき, G は単純群 (simple group) であると言う. □

[20] Abel 群の部分群は全て正規部分群であることを示せ. 正規ではない部分群の例を挙げよ. □

[21] 単純 Abel 群は単位群 $\{1\}$ または素数位数の巡回群である. □

単純 Abel 群はあまりにも単純過ぎてつまらないので, 単に単純群と言った場合には Abel 群を除く場合が多い.

[22] (核と像 (kernel and image)) 群の準同型 $f : G \to H$ について以下を示せ:

1. f の核 (kernel of f) を $\operatorname{Ker} f := f^{-1}(1) = \{\, x \in G \mid f(x) = 1 \,\}$ と定義する. $\operatorname{Ker} f$ は G の正規部分群である.
2. f の像 $\operatorname{Im} f := f(G)$ は H の部分群である. □

逆に群 G の任意の正規部分群は G から別の群へのある準同型写像の核に等しくなるであろうか? 以下のように答は肯定的である.

[23] (商群 (quotient group))) G は群であるとし, H はその正規部分群であるとし, $[x] := xH = Hx$ $(x \in G)$ と置く. このとき, $G/H = G\backslash H = \{\, [x] \mid x \in G \,\}$ であり, G/H に積を $[x][y] := [xy]$ $(x, y \in G)$ によって定義することができて, G/H が自然の群をなすことを示せ. この群 G/H を G の正規部分群 H による商群と呼ぶ. さらに, $p : G \to G/H$ を $p(x) = [x]$ $(x \in G)$ と定めると, p は全射準同型であり, $\operatorname{Ker} p = H$ が成立することを示せ. □

[24] (準同型定理 (homomorphsim theorem)) 群の準同型 $f : G \to H$ に対して, 群の同型写像 $\phi : G/\operatorname{Ker} f \to \operatorname{Im} f$ を $\phi([x]) = f(x)$ $(x \in G)$ と定めることができる. □

群 G からそれ自身への同型写像を G の自己同型 (automorphism) と呼ぶ. G の自己同型全体が写像の合成に関してなす群を $\operatorname{Aut} G$ と書き, G の**自己同型群 (automorphism group)** と呼ぶ. 準同型写像 $\sigma : G \to \operatorname{Aut} G$ を $\sigma(g)(x) = gxg^{-1}$ $(g, x \in G)$ と定めることができる. σ の $\operatorname{Aut} G$ における像を $\operatorname{Int} G$ と書き, G の**内部自己同型群 (inner automorphism group)** と呼ぶ. この σ は G の G 自身への左作用を定める. この作用に関する G 軌道を G の**共役類 (conjugate class)** と呼ぶ. すなわち, $x \in G$ の共役類とは

$$C_G(x) := \{\, gxg^{-1} \mid g \in G \,\}$$

のことである. G の 2 つの部分群 H, K がある $g \in G$ に関して $gHg^{-1} = K$ となっているとき, H と K は互いに共役であると言う.

[25] 以下を示せ:

1. $\operatorname{Int} G$ は $\operatorname{Aut} G$ の正規部分群である. $\operatorname{Aut} G$ の $\operatorname{Int} G$ による商群を $\operatorname{Out} G$ と書き, **外部自己同型群 (outer automorphism group)** と呼ぶ.
2. G が Abel 群であるための必要十分条件は G の全ての共役類が 1 点集合になっていることである.
3. G の部分群 H が正規であるための必要十分条件は H と共役な G の部分群が H 自身に限ることである. □

[26] 対称群 S_n の共役類と n の分割 (partition) は一対一に対応している. ここで, n の分割とは n を正の整数の和で表わすやり方のことである. 例えば, 4 の分割は $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ の 5 通りがある. □

ヒント: 任意の $\sigma \in S_n$ に対して, σ から生成される巡回群 σ の $A = \{1, 2, \ldots, n\}$ への作用による軌道分解を考えると, n の分割が得られ, 分割が等しい σ が互いに共役であることを示すことができる. σ が分割に応じた巡回置換の積で表示されることを示せ.

[27] 複素一般線形群 $GL_n(\mathbb{C})$ の共役類は対角成分に 0 を含まない Jordan 標準形で分類される. □

群 G の部分集合 A に対する A の**中心化群 (centralizer)** を

$$Z_G(A) := \{\, g \in G \mid ga = ag \ \forall x \in A \,\}$$

と定める. $Z(G) := Z_G(G)$ と G の**中心 (center)** と呼ぶ.
G の部分群 H に対して, H の**正規化群 (normalizer)** を

$$N_G(H) := \{\, g \in G \mid gH = Hg \,\}$$

と定める.

[28] 以下を示せ:

1. $Z(G)$ は G の可換な正規部分群である.
2. 自然な同型写像 $G/Z(G) \xrightarrow{\sim} \operatorname{Int} G$ が存在する.
3. H の正規化群 $N_G(H)$ は H を正規部分群として含むような G の最大の部分群である.
4. $N_G(H)$ は H に共役 $\sigma(g)(h) = ghg^{-1}$ $(g \in N_G(H),\ h \in H)$ によって作用する. この作用は準同型写像 $\sigma : N_G(H) \to \operatorname{Aut} H$ を与える. この準同型の核は H の中心化群 $Z_G(H)$ に等しい. □

3 群の例

3.1 行列群

[29] **(直交群)** ベクトル空間 $\mathbb{R}^n$ に通常の内積とノルムを

$$(x, y) := \sum_{i=1}^{n} x_i y_i \quad (x = (x_1, \ldots, x_n)^t, y = (y_1, \ldots, y_n)^t \in \mathbb{R}^n)$$
$$|x| := \sqrt{(x, x)} \quad (x = (x_1, \ldots, x_n)^t \in \mathbb{R}^n)$$

と入れておく. $\mathbb{R}^n$ からそれ自身へのベクトル空間として同型写像で内積を保つもの全体を $O(n)$ と書く:

$$O(n) := \{\, A \in GL_n(\mathbb{R}) \mid (Ax, Ay) = (x, y) \ \forall x, y \in \mathbb{R}^n \,\}.$$

このとき, 以下を示せ:

1. $GL_n(\mathbb{R})$ を可逆な n 次実正方行列全体のなす群と自然に同一視すれば,

$$O(n) = \{\, A \in GL_n(\mathbb{R}) \mid AA^t = A^tA = 1_n \,\}.$$

ここで, 1_n は単位行列である.

2. $O(n)$ は写像の合成もしくは行列の積に関して自然に群をなす. この $O(n)$ を n 次直交群 (orthogonal group) と呼ぶ.

3. 次が成立する:

$$O(n) = \{\, A : \mathbb{R}^n \to \mathbb{R}^n \mid A \text{ は線形でかつ } |Ax| = |x| \ \forall x \in \mathbb{R}^n \,\}.$$

ヒント: 内積をノルムで表示する式が存在する.

4. 行列式を取る写像を det と書くと, $\det : O(n) \to \mathbb{R}^\times$ は群の準同型であり, $\det O(n) = \{\pm 1\}$. $\det : O(n) \to \mathbb{R}^\times$ の核を $SO(n)$ と書き, n 次の特殊直交群 (special orthogonal group) と呼ぶ. □

[30] $SO(n)$ は位相空間として連結かつコンパクトであり, $O(n)$ はちょうど 2 つの連結成分に分かれる. □

ヒント: [佐武] p.178

[31] $SO(2)$ は次の形に書ける:

$$SO(2) = \left\{ \left. \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \right| \theta \in \mathbb{R} \right\}. \quad \square$$

[32] $SO(3)$ の共役類の代表系として,

$$\left\{ \left. \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \right| 0 \leqq \theta \leqq \pi \right\}$$

がとれる. すなわち, $O(3)$ の元はある軸を中心とした回転で表示可能である. □

[33] (ユニタリ群) ベクトル空間 $\mathbb{C}^n$ に通常の内積とノルムを

$$(x, y) := \sum_{i=1}^{n} \bar{x}_i y_i \quad (x = (x_1, \ldots, x_n)^t, y = (y_1, \ldots, y_n)^t \in \mathbb{C}^n)$$
$$|x| := \sqrt{(x, x)} \quad (x = (x_1, \ldots, x_n)^t \in \mathbb{C}^n)$$

と入れておく. $\mathbb{C}^n$ からそれ自身へのベクトル空間として同型写像で内積を保つもの全体を $U(n)$ と書く:

$$U(n) := \{\, A \in GL_n(\mathbb{C}) \mid (Ax, Ay) = (x, y) \ \forall x, y \in \mathbb{C}^n \,\}.$$

このとき, 以下を示せ:

1. $GL_n(\mathbb{C})$ を可逆な n 次複素正方行列全体のなす群と自然に同一視すれば,

$$U(n) = \{\, A \in GL_n(\mathbb{C}) \mid AA^* = A^*A = 1_n \,\}.$$

ここで, A^* は A を転置して複素共役を取って得られる行列であり, 1_n は単位行列である.

2. $U(n)$ は写像の合成もしくは行列の積に関して自然に群をなす. この $U(n)$ を n 次ユニタリ群 (unitary group) と呼ぶ.

3. 次が成立する:

$$U(n) = \{\, A : \mathbb{C}^n \to \mathbb{C}^n \mid A \text{ は線形でかつ } |Ax| = |x| \ \forall x \in \mathbb{C}^n \,\}.$$

ヒント: 内積をノルムで表示する式が存在する.

4. 行列式を取る写像を det と書くと, $\det : U(n) \to \mathbb{C}^\times$ は群の準同型であり, $\det U(n) = U(1) = \{\, x \in \mathbb{C} \mid |z| = 1 \,\}$. $\det : U(n) \to U(1)$ の核を $SU(n)$ と書き, n 次の特殊ユニタリ群 (special unitary group) と呼ぶ. □

[34] $U(n)$ と $SU(n)$ は連結かつコンパクトである. □

[35] $SU(2)$ は次のように書ける:

$$SU(2) = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \,\middle|\, z, w \in \mathbb{C} \text{ and } |z|^2 + |w|^2 = 1 \right\}. \quad \square$$

[36] $SU(2)$ は 3 次元球面 S^3 と同相である. □

[37] (三角行列のなす群) 体 K に対して, $GL_n(K)$ 内の上三角で対角線上の成分が全て 1 であるような行列全体の集合を $U_n(K)$ と書くと, $U_n(K)$ は $GL_n(K)$ の部分群である. しかし, $n \geqq 2$ ならば $GL_n(K)$ の正規部分群ではない. □

[38] (四元数体 (quaternion)) 次のように表示された 4 次元の実ベクトル空間を考える:

$$\mathbb{H} = \{\, a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}.$$

この 4 次元のベクトル空間に 1 が単位元になるような $\mathbb{R}$ 上の代数 (algebra) の構造を

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

という規則によって入れることができる. 以下を示せ:

1. 結合律が成立していることを確かめよ.

2. 0 以外の $\mathbb{H}$ の元は積に関して逆元を持つ. すなわち, $\mathbb{H}$ は斜体 (skew field) である. $\mathbb{H}$ は一般に四元数体 (quaternion) と呼ばれている.

3. 乗法群 $\mathbb{H}^\times$ は $SU(2) \times \mathbb{R}_{>0}$ に同型である. □

ヒント: $z = a + bi$, $w = c + di$ と置くと $a + bi + cj + dk = z + wj$.

[39] (有限体上の一般線形群の位数) $\mathbb{F}_q$ は位数 q の (すなわち q 個の元で構成される) 有限体であるとする. このとき, $GL_n(\mathbb{F}_q)$ は有限群になり, その位数は

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)(q - 1)$$

に等しい. $GL_n(\mathbb{F}_q)$ の部分群 $U_n(\mathbb{F}_q)$ の位数は $q^{n(n-1)/2}$ である. □

ヒント: $GL_n(K)$ と K^n の中の互いに一次独立な n 本のベクトルの組の全体のなす集合は自然に一対一に対応している. まず, 1 本目のベクトルは 0 以外のものを任意に選べる. 2 本目のベクトルは 1 本目のベクトルで張られる直線以外から選ばなければいけない. 3 本目のベクトルは 1 本目と 2 本目のベクトルで張られる平面以外から選ばなければいけない. ……

[40] 有限体の元の個数 q はある素数 p の正巾 p^e に等しい. □

[41] k が有限体であるとき, その乗法群 $k^\times$ は巡回群になる. □

[42] (特殊線形群) 体 K に対して, 行列式を取る写像 $\det : GL_n(K) \to K^\times$ は群の準同型写像であり, $\det GL_n(K) = K^\times$ である. $\det : GL_n(K) \to K^\times$ の核を $SL_n(K)$ と書き, 特殊線形群 (special linear group) と呼ぶ. 位数 q 有限体 $\mathbb{F}_q$ に対して, $SL_n(\mathbb{F}_q)$ の位数は,

$$q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)$$

に等しい. $SL_n(\mathbb{F}_q)$ の部分群 $U_n(\mathbb{F}_q)$ の位数は $q^{n(n-1)/2}$ である. □

3.2 自由群と基本関係式

[43] (自由群の構成) 集合 A は文字の集合であるとし, A^{-1} は x^{-1} $(x \in A)$ なる新しい文字全体の集合であるとし, A および A^{-1} の含まれる文字で構成された文字列 (すなわち文字を有限個横に並べたもの) 全体の集合を S と表わす:

$$S := \bigcup_{n=0}^{\infty} \{\, x_1 \cdots x_n \mid x_1, \ldots, x_n \in A \cup A^{-1} \,\}.$$

ただし, $n = 0$ には空の文字列が対応していると考え, 空の文字列を $\emptyset$ と書くことにする. 2 つの文字列を単に繋げるという 2 項演算を考えることによって, S には結合律を満たす積が定義され, 空文字列 $\emptyset$ はそ単位元をなす. $s = x_1 \cdots x_n \in S$ $(x_i \in A \cup A^{-1})$ の中の隣りあった $x_i x_{i+1}$ である aa^{-1} もしくは $a^{-1}a$ $(a \in A)$ に等しくなっている部分があるとき, その 2 文字を取り除いてできる文字列を t とし, $s \sim t$ と書くことにする. この関係 $\sim$ から生成される同値関係を $\approx$ とし[3], $G := S/\!\approx$ と置く. このとき, S における積が G に群の構造を自然に定めることを示せ. この G を**集合 A から生成される自由群 (free group generated by A)** と呼び, F_A と書くことにし, n 個の文字から生成された自由群を F_n と書くことにする. □

[3]第 1.2 節を見よ.

[44] **(部分集合から生成された (正規) 部分群)** 群 G の部分集合 A に対して以下を示せ:

1. A および A^{-1} の要素達の有限個の積全体のなす G の部分集合 H は G の部分群で A を含むものの中で最小である. H を A から生成される G の部分群と呼ぶ.
2. $\{\, gag^{-1} \mid a \in A,\ g \in G \,\}$ から生成される G の部分群 N は正規部分群であり A を含むものの中で最小である. N を A から生成される G の正規部分群と呼ぶ.

ただし 0 個の要素の積は単位元になると約束しておく. □

ヒント: G の部分集合 N が G の正規部分群であるための必要十分条件は, 1 を含み, 積と逆元で閉じていて, G の共役による作用でも閉じていることである.

[45] **(基本関係式)** 以下を示せ:

1. 集合 A から生成された自由群 F_A を考える. A の文字を F_A の対応する元に移す写像を $i : A \to F_A$ と書く. このとき, 任意の群 G と任意の写像 $f : A \to G$ に対して, $\phi \circ i = f$ を満たす準同型写像 $\phi : F_A \to G$ が唯一存在する.
2. もしも群 G が $A \subset G$ から生成されるならば, 上の ϕ によって G は A から生成される自由群 F_A の像になる. そのとき, 準同型定理によって, 同型 $G \cong F_A/\operatorname{Ker}\phi$ が成立する.

群 G が $A \subset G$ から生成されるとき, $R \subset F_A$ が生成する正規部分群が $\operatorname{Ker}\phi$ に一致するとき, $\{\, \text{“}r = 1\text{”} \mid r \in R \,\}$ を生成系 A に関する G の**基本関係式**と呼ぶ. これは右辺が単位元の等式の集合であるが, 右辺が単位元でない場合は右辺の逆元を両辺にかけて右辺を単位元の等式に直せるので, 右辺が単位元でない等式を関係式として考えても良い. □

[46] 群と写像の組 $(F, \iota : A \to F)$ が上の問題の $(F_A, i : A \to F_A)$ と同じ性質を持つならば F は自由群 F_A に同型である. □

[47] 複素平面 $\mathbb{C}$ から互いに異なる n 個の点を取り除いてできる位相空間を X とし, 任意に $x_o \in X$ を取る. このとき, X の基本群 $\pi_1(X, x_0)$ は n 個の元から生成された自由群 F_n に同型である. □

[48] 向き付け可能なジーナス g の閉曲面の基本群は, $a_1, \ldots, a_g, b_1, \ldots, b_g$ から生成され, 基本関係式 $a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1} = 1$ を持つ群に同型である. □

3.3 対称群

[49] **(一般線形群と対称群の関係)** $G = GL_n(K)$ 内の対角行列全体のなす部分群を $T = T_n(K)$ と書くことにする. T の G における中心化群 $Z_G(T)$ と正規化部分群を $N_G(T)$ を考える. このとき, $Z_G(T) = T$ であり, $N_G(T)/T$ は対称群 $W = S_n$ に同型である. □

ヒント: 任意の $x \in N_G(T)$ の T への共役による作用は T の対角成分のある置換になり, 任意の置換がそのようにして得られる.

参考: この結果は簡約代数群 (reductive algebraic group) とその Weyl 群の関係に一般化される. $GL_n(K)$ は簡約代数群の最もわかり易い例であり, 対称群 S_n は Weyl 群の最もわかり易い例である.

[50] n 次対称群 S_n の生成系として, $s_i = (i, i+1)$ $(i = 1, \ldots, n-1)$ が取れ, それらは以下の関係式を満たしている:

(a) $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \quad (i = 1, \ldots, n-2)$,

(b) $s_i s_j = s_j s_i \quad (|i-j| \geqq 2)$,

(c) $s_i^2 = 1 \quad (i = 1, \ldots, n-1)$. □

[51] 上の問題の (a), (b), (c) は生成系 $\{s_1, \ldots, s_{n-1}\}$ に関する S_n の基本関係式である. □

参考: $\{s_1, \ldots, s_{n-1}\}$ から生成される群で (a), (b) を基本関係式とする群は組紐群 (くみひも群, braid group) と呼ばれている. 同様に対称群は阿弥陀籤群 (あみだくじ群) と呼ぶべきかもしれない[4].

[52] 対称群 S_n の元 σ が, 互換の積で表わされているとき, そこに登場する互換が偶数個か奇数個かは表示によらずに決まっている. 偶数のとき σ は偶置換であると言い, 奇数のとき奇置換であると言う. $\mathrm{sgn} : S_n \to \{\pm 1\}$ を σ が偶置換なら $\mathrm{sgn}(\sigma) = 1$, 奇置換なら $\mathrm{sgn}(\sigma) = -1$ と定めると, sgn は群の準同型写像をなす. sgn の核を A_n と書き, n 次**交代群 (alternating group)** と呼ぶ. □

ヒント: 差積 $\prod_{i<j}(x_i - x_j)$ への作用を調べる.

[53] 以下を示せ:

1. 3 次の交代群 A_3 は位数 3 の巡回群である.
2. $n \geqq 3$ のとき, n 次交代群 A_n は長さ 3 の巡回置換で生成される.
3. 4 次の交代群 A_4 は位数 4 の Abel 正規部分群 V を持ち, V による剰余群は位数 3 の巡回群になる.
4. $n \geqq 4$ のとき, n 次交代群 A_n は非 Abel 群である.
5. $n \neq 4$ ならば n 次交代群 A_n は単純群である. □

4 群の様々な積

4.1 直積

[54] (群の直積) 任意の $a \in A$ に対して群 G_a が対応しているとする. このとき, 集合としての直積

$$G := \prod_{a \in A} G_a := \{\, (x_a)_{a \in A} \mid x_a \in G_a \ (a \in A) \,\}$$

は成分ごとに積を

$$(x_a)_{a \in A}(y_a)_{a \in A} = (x_a y_a)_{a \in A} \quad (x_a, y_a \in G_a)$$

[4]演習の時間に絵を書いて, これらの理由を説明する予定である.

と定めることによって自然に群をなす. これを群の直積と呼ぶ. 任意の $a \in A$ に対して, 標準的な射影 (canonical projection) $p_a : G \to G_a$ を

$$p_a\left((x_a)_{a\in A}\right) := x_a \quad (x_a \in G_a)$$

と定めると p_a は群の準同型写像である. 任意の群 H と準同型写像の族 $\{f_a : H \to G_a\}_{a\in A}$ に対して, 直積群への準同型写像 $\phi : H \to G$ で

$$p_a \circ \phi = f_a \quad (a \in A)$$

をみたすものが唯一存在する. この結果を直積 $(G, \{p_a\})$ の普遍性 (universality) という. さらに, $(H, \{f_a\})$ も普遍性の条件を満たしていれば, 上の ϕ は同型写像になる. □

[55] (剰余群を取る操作と直積の可換性) 任意の $a \in A$ に対して, G_a は群であり, N_a はその正規部分群であるとする. このとき, 次の同型が自然に成立している:

$$\left(\prod G_a\right) \Big/ \left(\prod N_a\right) \cong \prod (G_a/N_a). \quad \square$$

ヒント: 自然な準同型写像たち $\prod G_a \to G_a \to G_a/N_a$ の合成を考えると, 直積の普遍性より, 準同型写像 $\prod G_a \to \prod (G_a/N_a)$, $(x_a) \mapsto (x_a N_a)$ が自然に定まる. これが全射でかつその核が $\prod N_a$ であることを示し, 準同型定理を適用せよ.

[56] (直積の判定法) G は群であり, $G_1, \ldots, G_n$ はその部分群であるとする. このとき, $\phi : \prod_{i=1}^n G_i \to G$, $(x_i)_{i=1}^n \mapsto x_1 \cdots x_n$ が同型写像をなすための必要十分条件は以下が成立することである:

1. $G_1, \ldots, G_n$ の各々は G の正規部分群である.
2. $G_1 \cdots G_n = G$.
3. 任意の $\nu = 1, \ldots, n-1$ に対して, $(G_1 \ldots G_\nu) \cap G_{\nu+1} = \{1\}$.

このとき, 自然に $G \cong \prod_{i=1}^n G_i$ が成立するという. □

[57] 0 でない複素数全体のなす乗法群 $\mathbb{C}^\times$ は絶対値が 1 の複素数全体のなす部分群 $U(1)$ と正の実数全体のなす乗法群 $\mathbb{R}_{>0}$ を含む. このとき, 自然に $\mathbb{C}^\times \cong U(1) \times \mathbb{R}_{>0}$ が成立している. □

[58] 四元数体 $\mathbb{H}$ の乗法群 $\mathbb{H}^\times$ は $SU(2)$ に同型な部分群と正の実数全体のなす乗法群 $\mathbb{R}_{>0}$ を含んでいる. このとき, 自然に $\mathbb{H}^\times \cong SU(2) \times \mathbb{R}_{>0}$ が成立している.

[59] 直積群 $G = H \times K$ の任意の部分群 G_1 について, $H \times \{1\} \subset G_1$ ならば K のある部分群 K_1 が存在して $G_1 = H \times K_1$ となる. □

[60] H, K は有限群であり, それらの位数は互いに素であると仮定する. このとき, 直積群 $G = H \times K$ の任意の部分群 G_1 に対して, 部分群 $H_1 \subset H$, $K_1 \subset K$ で $G_1 = H_1 \times K_1$ となるものが存在する.

[**61**] **(直積因子)** G は群であり, H はその部分群であるとする. G のある部分群 K が存在して自然な同型 $G \cong H \times K$ が成立するとき, H は G の直積因子であるという. H が G の直積因子ならば H は G の正規部分群である. G の正規部分群 H に対して, 以下の条件は互いに同値である:

1. H は G の直積因子である.
2. 準同型写像 $p_H : G \to H$ で $p_H \circ i_H = \mathrm{id}_H$ を満たすものが存在する. ここで, i_H は自然な入射 $H \to G$ である.
3. 準同型写像 $i_{G/H} : G/H \to G$ で $p_{G/H} \circ i_{G/H} = \mathrm{id}_{G/H}$ でかつ $\mathrm{Im}\, i_{G/H}$ が G の正規部分群になるものが存在する. ここで, $p_{G/H}$ は自然な射影 $G \to G/H$ である. □

[**62**] 素因数分解された正の整数 $n = p_1^{e_1} \cdots p_\nu^{e_\nu}$ に対して, 加法群として,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\nu^{e_\nu}\mathbb{Z}. \quad \square$$

[**63**] **(直既約)** 群 G が G と $\{1\}$ 以外の正規部分群を持たないとき, G は**単純 (simple)** であるという. 群 G が G と $\{1\}$ 以外の直積因子を持たないとき, G は**直既約 (indecomposable)** であるという. 以下を示せ:

1. 単純群は直既約である.
2. 素数 p と正の整数 e に対して, 位数 p^e の巡回群は直既約である.
3. 素数以外の 4 以上の整数 n に対して, 位数 n の巡回群は単純ではない. □

4.2 Abel 群の直和

[**64**] **(Abel 群の直和)** 任意の $a \in A$ に対して加法 Abel 群 M_a が対応しているとする. このとき, 群の直積 $\prod_{a\in A} M_a$ は Abel 群をなす. $\{M_a\}$ の直和を次のように定める:

$$M := \bigoplus_{a\in A} M_a := \left\{ (x_a)_{a\in A} \in \prod M_a \,\middle|\, \text{有限個を除いて } x_a = 0 \right\}.$$

これは自然に $\prod_{a\in A} M_a$ の部分群をなす. これを Abel 群の直和と呼ぶ. 標準的な入射 (canonical inclusion) $i_a : M_a \to M$ を

$$i_a(x_a) := (\delta_{a,b} x_a)_{b\in A} \quad (x_a \in G_a)$$

と定める. ここで, $\delta_{a,b}$ は Kronecker のデルタである. すなわち, $a = b$ のとき $\delta_{a,b} = 1$ で, そうでないとき $\delta_{a,b} = 0$. このとき, i_a は群の準同型写像である. 任意の Abel 群 N と準同型写像の族 $\{f_a : M_a \to N\}_{a\in A}$ に対して, Abel 群の直和からの準同型写像 $\phi : M \to N$ で

$$\phi \circ i_a = f_a \quad (a \in A)$$

をみたすものが唯一存在する. この結果を Abel 群の直和 $(M, \{i_a\})$ の普遍性 (universality) という. さらに, $(N, \{f_a\})$ も普遍性の条件を満たしていれば, 上の ϕ は同型写像になる. □

[65] **(剰余群を取る操作と直和の可換性)** 任意の $a \in A$ に対して, M_a は加法 Abel 群であり, N_a はその部分群であるとする. このとき, 次の同型が自然に成立している:

$$\left(\bigoplus M_a\right) \Big/ \left(\bigoplus N_a\right) \cong \bigoplus (M_a/N_a). \quad \square$$

ヒント: 準同型写像 $\bigoplus G_a \to \bigoplus (G_a/N_a)$, $(x_a) \mapsto (x_a N_a)$ が well-defined であることおよびそれが全射でかつその核が $\bigoplus N_a$ に等しいことを示し, 準同型定理を適用せよ.

[66] 体 K 上の 1 次元のベクトル空間の族 $\{Ke_a\}_{a\in A}$ の直和 $V = \bigoplus_{a\in A} Ke_a$ は自然に K 上ベクトル空間とみなせ, その基底として $\{e_a\}_{a\in A}$ が取れることを示せ. ここで, e_a と $(\delta_{a,b}e_a)_{b\in A} \in V$ を同一視した. $\square$

4.3 自由積

[67] **(自由積)** 任意の $a \in A$ に対して群 G_a が対応しているとする. このとき, 次の性質を満たす群 G と準同型写像の族 $\{i_a : G_a \to G\}_{a\in A}$ が存在する: 任意の群 H と準同型写像の族 $\{f_a : G_a \to H\}_{a\in A}$ に対して, 準同型写像 $\phi : G \to H$ で $\phi \circ i_a = f_a$ $(a \in A)$ を満たすものが唯一存在する. このような群 G は同型を除いて唯一定まり, $\{G_a\}$ の**自由積 (free product)** もしくは **余積 (coproduct)** と呼ばれている. 群 H, K の自由積を $H * K$ と書く. $\square$

[68] 上の問題の結果を認めた上で, 自由積 $\mathbb{Z} * \mathbb{Z}$ が 2 つの文字から生成される自由群に同型であることを示せ. $\square$

4.4 制限直積

[69] **(制限直積)** 任意の $p \in P$ に対して G_p は群であり, K_p はその部分群であるとする. このとき, 直積群 $\prod G_p$ の部分群を

$$\prod{}' G_p := \left\{ (x_p)_{p\in P} \in \prod G_p \,\middle|\, \text{有限個を除いて } x_p \in G_p \right\}.$$

によって定めることができる. これを $\{(G_p, K_p)\}$ の制限直積と呼ぶ. $\square$

参考 各素数 p に対して p 進体 $\mathbb{Q}_p$ という $\mathbb{Q}$ を含む体と p 進整数環 $\mathbb{Z}_p$ という $\mathbb{Z}$ を含み $\mathbb{Q}_p$ に含まれる可換環が存在する. $\mathbb{Q}_p$ は数論的には実数体 $\mathbb{R}$ と同等に扱われるべき体である. P を素数全体に ∞ という文字を付け加えた集合であるとし, 素数 p に対して $G_p := GL_n(\mathbb{Q})$, $G_\infty := GL_n(\mathbb{R})$ と置き, それらの部分群を $K_p := GL_n(\mathbb{Z}_p)$, $K_\infty := O(n)$ と定めておく. このとき, $\{(G_p, K_p)\}_{p\in P}$ の制限直積

$$GL_n(\mathbb{A}) = GL_n(\mathbb{R}) \times \prod{}' GL_n(\mathbb{Q}_p)$$

を $GL_n(\mathbb{Q})$ のアデール群と呼ぶ. 特に $GL_1(\mathbb{A})$ を $\mathbb{Q}$ のイデール群と呼ぶ. これらは数論で極めて重要な役目を果たす.

4.5 半直積

[70] (半直積) E を群とし, N をその正規部分群であるとし, $G = E/N$ と置き, 自然な写像を $i_N : N \to E$, $p_G : E \to G$ と書くことにする. このとき, 以下の条件は互いに同値である:

1. 準同型写像 $i_G : G \to E$ で $p_G \circ i_G = \mathrm{id}_G$ を満たすものが存在する.
2. E の部分群 G' で $E = G'N$, $G' \cap N = \{1\}$ をみたすものが存在する.
3. E の部分群 G' が存在して, 任意の $x \in E$ は $x = gn$, $g \in G'$, $n \in N$ と一意的に表わされる.

このとき, E を G と N の**半直積 (semi-direct product)** と呼び, $E = G \ltimes N$ と書く[5]. 自然な射影 p_G を通して, $i_G(G)$ と G' は G と同型である. E の群の演算は $x, y \in E$ を $x = hn$, $y = gm$ $(g, h \in G', m, n \in N)$ と表わすとき,

$$xy = hngm = hg(g^{-1}ng)m, \quad (g^{-1}ng)m \in N, hg \in G'$$

と書けるので, G' と N の群構造と G' の N への左作用 $n \mapsto g(n) = gng^{-1}$ から決定される. □

[71] (半直積の作り方) G と N は群であり, 準同型写像 $\sigma : G \to \mathrm{Aut}\, N$ が与えられていると仮定し, $g(n) = \sigma(g)(n)$ $(g \in G, n \in N)$ と書くことにする. このとき, 集合としての直積 $E = G \times N$ に,

$$(h, n)(g, m) = (hg, g^{-1}(n)m) \quad (m, n \in N, g, h \in G)$$

によって積を入れると, E は自然に群をなし, G と N の半直積をなす. □

[72] (アフィン変換群) 任意の体 K に対して, $GL_n(K)$ の K^n への作用は半直積 $GL_n(K) \ltimes K^n$ を定める. これを体 K 上のアフィン変換群と呼ぶ. アフィン変換群 $GL_n(K) \ltimes K^n$ は

$$(g, u)v := g(u + v) \quad (g \in GL_n(K), u, v \in K^n)$$

によって, 集合 K^n に自然に作用している. □ □

[73] (Euclid 変換群) 直交群 $O(n)$ の $\mathbb{R}^n$ への自然な作用は半直積 $O(n) \ltimes \mathbb{R}^n$ を定める. これを $\mathbb{R}^n$ の Euclid 変換群と呼ぶ. Euclid 変換群 $O(n) \ltimes \mathbb{R}^n$ は

$$(g, u)v := g(u + v) \quad (g \in GL_n(K), u, v \in K^n)$$

によって, 集合 $\mathbb{R}^n$ に自然に作用している. そして, この作用は $\mathbb{R}^n$ における自然な距離 $d(v, w) = ||v - w||$ $(v, w \in \mathbb{R}^n)$ を保つ. ここで, $||\cdot||$ は $\mathbb{R}^n$ の通常の Euclid ノルムである. □

[5] $E \triangleright N$ (N は E の正規部分群) という記号法と整合的であることに注意すると覚え易い.

[74] **(A_{n-1} 型の拡張アフィン Weyl 群の定義)** S_n は A_{n-1} 型の Weyl 群と呼ばれる場合がある. 成分の置換によって, 対称群 S_n は $\mathbb{Z}^n$ に自然に作用する. この作用が定める半直積 $S_n \ltimes \mathbb{Z}^n$ を A_{n-1} 型の拡張アフィン Weyl 群と呼ぶことがある. これらは自然に Euclid 変換群の部分群とみなされる. □

[75] **(A_1 型の拡張アフィン Weyl 群の生成元)** $S_2 \ltimes \mathbb{Z}^2$ が以下の元から生成されることを示せ:

$$s_1 = (1,2), \quad s_0 = (1,-1)^t(1,2), \quad \omega = (1,0)^t(1,2).$$

ここで, S_2, $\mathbb{Z}^2$ と $S_2 \times \{1\}$, $\{1\} \times \mathbb{Z}^2$ のそれぞれを同一視し, $\mathbb{Z}^2$ の元は $(a,b)^t$ と表わした. (i,j) は i と j の互換である. s_1, s_0, ω が平面のどのような変換になっているかを図を描いて説明せよ. □

[76] **(A_n 型の拡張アフィン Weyl 群の生成元)** $G = S_n \ltimes \mathbb{Z}^n$ と置く. G は以下の元から生成される:

$$\begin{aligned} s_i &= (i, i+1) \qquad \text{for } i = 1, \ldots, n-1, \\ s_0 &= (1, 0, \ldots, 0, -1)^t(1, n), \\ \omega &= (1, 0, 0, \ldots, 0)^t(1, 2, \ldots, n). \end{aligned}$$

ここで, S_n, $\mathbb{Z}^n$ と $S_n \times \{1\}$, $\{1\} \times \mathbb{Z}^n$ のそれぞれを同一視し, $\mathbb{Z}^n$ の元は $(a_1, \ldots, a_n)^t$ と表わした. (i,j) は i と j の互換であり, $(1,2,\ldots,n)$ は $1 \mapsto 2 \mapsto \cdots \mapsto n \mapsto 1$ という巡回置換である. □

5 有限群の話

5.1 基本的な話

[77] G が有限群のとき, 以下が成立する:

1. G は集合 X に作用しているとする. 任意の $x \in X$ に対して,

   $$|G_x||Gx| = |G|.$$

   ここで, Gx は x の G 軌道であり, G_x は x を固定する元全体のなす G の等方部分群 (x の固定化部分群) である.

2. G 軌道全体の集合を $X\backslash G = \{\, Gx \mid x \in X \,\}$ と書くのであった. X が有限集合であれば

   $$|X| = \sum_{O \in G\backslash X} |O|.$$

3. さらに, $G\backslash X$ の完全代表系 $\{x_1, \ldots, x_n\} \subset X$ を取ると,

   $$|X| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}.$$

4. G の部分群 H に対して,
$$|G| = |G/H||H|.$$
特に $|H|$ は $|G|$ の約数である (Lagrange). $|G/H|$ を H の G における**指数 (index)** と呼び, $(G : H)$ と書く.

5. G の共役類全体の集合 $C(G) = \{ C_G(x) \mid x \in G \}$ を考える. (ここで $C_G(x) := \{ gxg^{-1} \mid g \in G \}$.) このとき,
$$|G| = \sum_{C \in C(G)} |C|.$$

6. $C(G)$ の完全代表系 $\{x_1, \ldots, x_n\} \subset G$ を取ると,
$$|G| = \sum_{i=1}^{n} \frac{|G|}{|Z_G(x_i)|}.$$
ここで $Z_G(x) := \{ g \in G \mid gx = xg \}$. これを**類等式**という. □

[**78**] **(Fermat)** 以下を示せ:

1. 有限群 G とその任意の元 a に対して $a^{|G|} = 1$.

2. 正の整数 n に対して, $\mathbb{Z}/n\mathbb{Z}$ は自然に可換環をなす.

3. 一般に可換環 R に対して,
$$R^\times := \{ a \in R \mid a \text{ は } R \text{ の中で掛け算に関する逆元を持つ} \}$$
と定めると, $R^\times$ は Abel 群をなす.

4. $\bar{a} = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ $(a \in \mathbb{Z})$ と置く. $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ であるための必要十分条件は a が n と互いに素なこと (すなわち $(a, n) = 1$) である.

5. Euler の函数を $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ と定めると, 任意の $a \in \mathbb{Z}$ に対して, $(a, n) = 1$ ならば $a^{\varphi(n)} \equiv 1 \mod n$. □

[**79**] Euler の函数 $\varphi(n)$ は以下のようにして計算される:

1. 素数 p と正の整数 e に対して, $\varphi(p^e) = p^{e-1}(p-1)$.

2. 素因数分解された正の整数 $n = p_1^{e_1} \cdots p_\nu^{e_\nu}$ に対して, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\nu^{e_\nu}\mathbb{Z}$ なる可換環の同型が存在する.

3. よって, $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_\nu^{e_\nu})$. □

[**80**] **(Sylow)** 一般に位数が素数 p の巾であるような有限群を p **群 (p-group)** と呼ぶ. G は有限群であるとし, G の位数を割る最大の p の巾は p^e であると仮定する. このとき, 位数 p^e の G の部分群を G の **Sylow p 部分群 (Sylow p-subgroup)** と呼ぶ. Sylow p 部分群に関して以下が成立する:

1. 任意の素数 p に対して Sylow p 部分群が存在する.
2. G の任意の p 部分群はある Sylow p 部分群に含まれている.
3. G の Sylow p 部分群は互いに共役である.
4. Sylow p 部分群の個数は p を法として 1 に合同である. □

ヒント: $n := |G| = p^e m$, $(p, m) = 1$ と置く.

まず, $(x+1)^{p^e m} \equiv (x^{p^e}+1)^m \mod p$ を示すことによって, 二項係数に関して, $\binom{n}{p^e} = \binom{p^e m}{p^e} \equiv m \mod p$ が成立していることを示せ.

Sylow p 部分群の存在は以下のようにして示される. $X := \{ S \subset G \mid |S| = p^e \}$ と置く. G を X に $g \cdot S := \{ gs \mid s \in S \}$ $(g \in G, S \in X)$ と作用させることができる. $|X| = \binom{n}{q} \equiv m \mod p$ なので $|X|$ は p と互いに素である. よって, ある $S \in X$ が存在して, S の G 軌道の元の個数 $|G \cdot S|$ は p と互いに素になる. このとき, S の等方部分群 $P := G_S$ が G の Sylow p 部分群であることがわかる. 実際, $|G \cdot S| = |G|/|P|$ は p と互いに素なので, $|P| = p^e$ でなければいけない.

残りは以下のようにして証明される. P を G の任意の Sylow p 部分群とし, $Y := \{ gPg^{-1} \mid g \in G \}$ と置く. Y は P と共役な Sylow p 部分群全体の集合である. p 部分群 H を Y に $h \cdot P' := hP'h^{-1}$ $(h \in H, P' \in Y)$ によって作用させることができる. この作用の H 軌道の含む元の個数は $|H|$ の約数なので p の巾である. 一方, $|Y| = |G|/|N_G(P)|$ であり, P は $N_G(P)$ の部分群なので, $|Y|$ は $|G|/|P| = m$ の約数になり, p と互いに素である. よって, ある $P' \in Y$ が存在して P' は H の作用で固定される. そのとき, $H \subset N_G(P')$ であるので, P' が $N_G(P')$ の正規部分群であることに注意すると HP' は G の部分群になることがわかる. HP' の位数は $|H||P'|$ の約数になるので, p の巾である. しかし, $|HP'| \leqq p^e$ でなければいけないので, $H \subset P'$ であることがわかる. H として Sylow p 部分群と取れば, ある $P' \in Y$ が存在して $H = P'$ であることがわかる. $H = P$ と取ったとき, Y への作用の不動点は P に限るので, $|Y|$ は p を法として 1 に等しいことがわかる.

[81] 標数 $p > 0$ の有限体 $\mathbb{F}_q$ について, 有限群 $G = GL_n(\mathbb{F}_q)$ を考える. 対角線が成分が全て 1 で下三角成分が全て 0 であるような行列からなる G の部分群は Sylow p 部分群である. □

[82] (正規部分群と剰余群の Sylow p 部分群) 有限群 G とその Sylow p 部分群 P を考える. このとき, G の正規部分群 N に対して, $P \cap N$ は N の Sylow p 部分群であり, PN/N は G/N の Sylow p 部分群である. □

[83] (Frattini) 有限群 G とその正規部分群 H と H の Sylow p 部分群 Q に対して, $G = N_G(Q)H$. □

[84] 素数 p について位数 p^2 の群は Abel 群になる. □

[85] 素数 p, q $(p > q)$ について位数 pq の群の構造を決定せよ. □

5.2 有限群の世界

この節はお話である. 以下, 群 G の部分群 H が G の正規部分群であるとき, $G \triangleright H$ と書くことにする. 有限群 G に対して, $G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_{n+1} = \{1\}$, $G_i \neq G_{i+1}$ を満たす部分群の列でこれ以上細分できないものを G の**組成列 (composition series)** と呼ぶ. **組成剰余群 (composition factor)** $F_i = G_i/G_{i+1}$ $(i = 1, \ldots, n)$ は単純群になる. **Jordan-Hölder の定理**より, 組成剰余群の全体は順序を除けば組成列の取り方によらないことが知られている.

これによってわかることは, 任意の有限群は幾つかの有限単純群を適切に組成列の形でうまいこと組み合わせることによって構成されるということだ.

したがって, 有限群の世界がどうなっているかを知るためには, まず, 有限単純群の分類が重要でかつ基本的な問題だということになる. この問題は前世紀の数学の発展によって解決されている.

参考文献

[群と加群] 堀田良之: 代数入門 — 群と加群 —, 数学シリーズ, 裳華房 1987

[十話] 堀田良之: 加群十話 — 代数学入門 —, すうがくぶっくす 3, 朝倉書店 1988

[佐武] 佐武 一郎: 線型代数学, 数学選書 1, 裳華房

[Shaf] I. R. Shafarevich: Basic Notions of Algebra, Encyclopaedia of Mathematical Sciences, Softcover Series Vol. 11, Springer 1997