第1章　群の基礎（解答編）

群論の基礎に関する参考書：
浅野啓三・永尾汎「群論」（岩波全書）
永尾汎「代数学」（朝倉書店）
松村英之「代数学」（朝倉書店）
ブルバキ「数学原論」（東京図書）

1.1　2項演算

- 2項演算：集合 A 上の2項演算とは、写像 $\mu : A \times A \to A$ のことである。$\mu(x,y)$ のことを $x \cdot y$ と略記する。
- 結合則：$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ が全ての A の要素 x, y, z について成立するとき、この2項演算は「結合則」を満たすという。
- 交換則：$x \cdot y = y \cdot x$ が全ての A の要素 x, y について成立するとき、この2項演算は「交換則」を満たす、または「可換な2項演算である」という。交換則を満足しない2項演算は、「非可換である」と言うことも多い。
- 単位元：A の中にある特別な元 e があって、$x \cdot e = e \cdot x = x$ が全ての A の要素 x について成立するとき、この元 e を2項演算の単位元とよぶ。　単位元は存在しないかもしれない。
- 逆元：A 上に単位元 e をもつ2項演算があるとき、元 $x \in A$ に対して、$xy = yx = e$ となる y のことを x の逆元であるという。任意の x に対して必ずしも逆元があるとは限らない。x の逆元 y が存在して一意的であるとき、$y = x^{-1}$ と書くことが多い。

問題 1.1.1 次のようにして集合 A 上に与えられた2項演算について、結合則、交換則が成り立つかどうか判定せよ。

(1) $A = \mathbf{R}$ として、2項演算を $x \cdot y = xy + x + y$ と定める。
解答). $\mathbf{R} \ni \forall x, y, z$ に対して, 結合則 : $((x \cdot y) \cdot z) = (xy+x+y) \cdot z = (xy+x+y)z+(xy+x+y)+z = x(yz+y+z)+x+(yz+y+z) = x \cdot (yz+y+z) = (x \cdot (y \cdot z))$. 交換則 : $x \cdot y = xy+x+y = yx+y+x = y \cdot x$. 単位元 : 0. 逆元 : $\frac{-x}{x+1} (x \neq -1)$.

(2) $A = \mathbf{N}$ として、2項演算を $x \cdot y =$「x と y の最大公約数」と定める。
解答). 交換則 : 定義より成立. 結合則 : $\mathbf{N} \ni \forall x, y, z$ に対して, $\gcd(x, y, z) =: d$, $\gcd(x, y) =: d_1$, $\gcd(d_1, z) =: d_2$, i.e. $\exists k_1, k_2, l_1, l_2 \in \mathbf{Z}$ $s.t.$ $d_1 = k_1 x + k_2 y$, $d_2 = l_1 d_1 + l_2 z$. d_1 を代入すると

$d_2 = l_1k_1x + l_1k_2y + l_2z$, i.e. $d_2 \geq d$. 一方, $\exists m_1, m_2, m_3, \in \mathbf{Z}$ $s.t.$ $d = m_1x + m_2y + m_3z$.
また, $\exists m, \in \mathbf{Z}$ $s.t.$ $md_1 = m_1x + m_2y$. md_1 を代入すると $d = md_1 + m_3z$, i.e. $d \geq d_2$. 以上のことより, $d = d_2$. $\gcd(x, y, z) = \gcd((x, y), z)$. 同様に, $\gcd(x, y, z) = \gcd(x, (y, z))$. 単位元：gcd(a,b)=a なる b に対して, gcd(c,b)=1 となる c がとれる. よって, なし. 逆元：なし.

(3) $A = \mathbf{N}^2$ として、$(a, b), (c, d) \in A$ に対して、$(a, b) \cdot (c, d) = (ad + bc, bd)$ と定義する。
解答). $A \ni \forall (a, b), (c, d), (e, f)$ に対して, 結合則：$((a, b) \cdot (c, d)) \cdot (e, f) = (ad + bc, bd) \cdot (e, f) = ((ad + bc)f + bde, bdf) = (adf + b(cf + de), bdf) = (a, b) \cdot (cf + de, df) = (a, b) \cdot ((c, d) \cdot (e, f))$. 交換則：$(a, b) \cdot (c, d) = (ab + dc, bd) = (cb + da, db) = (c, d) \cdot (a, b)$. 単位元：$ab + bc = a, bd = b$ とすると, $d = 1, bc = 0$. よって, なし. 逆元：なし.

(4) X を集合、A を X の全ての部分集合の集合とする（$A = 2^X$）。このとき、$x, y \in A$ に対して、$x \cdot y = x \cap y$ と定義する。
解答). 結合則：$x \cdot (y \cdot z) = x \cdot (y \cap z) = x \cap (y \cap z) = (x \cap y) \cap z = (x \cdot y) \cdot z$. 交換則：$x \cdot y = x \cup y = y \cup x = y \cdot x$. 単位元：$A$. 逆元：$A$ は逆元を持ちその逆元は, A.

(5) A を平面上の全ての点の集合とする。このとき、$x \cdot y =$「x と y を結ぶ線分の中点」と定義する。
解答). $A \times A \ni (x_1, y_1), (x_2, y_2), (x_3, y_3)$ に対して, 結合則：$((x_1, y_1)(x_2, y_2))(x_3, y_3) = (\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2})(x_3, y_3) = (\frac{x_1+x_2+2x_3}{4}, \frac{y_1+y_2+2y_3}{4}), (x_1, y_1)((x_2, y_2)(x_3, y_3)) = (x_1, y_1)(\frac{x_2+x_3}{2}, \frac{y_2+y_3}{2}) = (\frac{2x_1+x_2+x_3}{4}, \frac{2y_1+y_2+y_3}{4})$. よって, 結合則は, 不成立. 交換則: $(x_1, y_1)(x_2, y_2) = (\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}) = (\frac{x_2+x_1}{2}, \frac{y_2+y_1}{2}) = (x_2, y_2)(x_1, y_1)$. 単位元：なし. 逆元：なし.

(6) Y を a から z までのアルファベットと空白 ( ) 、コンマ (,) 、ピリオド (.) からなる集合とし、A を Y の要素を有限個並べて得られる列の集合とする。たとえば、$(you\ are\ stupid, but\ i\ am\ not.) \in A$ である。二つの A の元 $\xi = (\alpha_1\alpha_2 \ldots \alpha_n)$ と $\xi' = (\alpha'_1\alpha'_2 \ldots \alpha'_m)$ は、$n = m$ で $\alpha_i = \alpha'_i$ $(1 \leqq i \leqq n)$ となるときに等しいとする。ここで、2 項演算を $\xi \cdot \xi' = (\alpha_1\alpha_2 \ldots \alpha_n\ \ \alpha'_1\alpha'_2 \ldots \alpha'_m)$ と 2 つの列を空白を一つはさんで連結することによって定義する。
解答). $A \ni a, b, c$ に対して, 結合則：$a \cdot (b \cdot c) = a \cdot (bc) = abc = (ab) \cdot c = (a \cdot b) \cdot c$. 交換則：$a \cdot b = ab, ba = b \cdot a$. 単位元：なし. 逆元：なし.

(7) 複素数係数の n 次正方行列の全体の集合 $A = M_{n\times n}(\mathbf{C})$ において、$x \cdot y$ を普通の行列の積として定義する。
解答). 2×2 行列で行う. (一般性は失わない.) 結合則：

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}$$
$$= \begin{pmatrix} i(ae+bg)+k(af+bh) & j(ae+bg)+l(af+bh) \\ i(ce+dg)+k(cf+dh) & j(ce+dg)+l(cf+dh) \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gi+hl \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}\right).$$

交換則：

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

単位元：

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

逆元：$\det A \neq 0$ なる A に対しては, 存在.

(8) 実数係数の n 次正方行列の全体の集合 $A = M_{n\times n}(\mathbf{R})$ において、 $x \cdot y = xy - yx$ と定義する。

解答). 結合則：なし. 例えば,

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right) \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

一方,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

交換則：$xy - yx \neq yx - xy$. 単位元：なし. e を単位元とする. $x \in A$ に対して, $x \cdot e = xe - ex = e \cdot x = ex - xe = x$. $x = xe - ex = xe - x - xe = -x$. よって, $2x = 0$, $i.e.$ $x = 0$.

逆元：なし.

(9) A を集合 X からそれ自身への全単射の全部の集合とする。このとき、2 項演算 $x \cdot y$ を写像の合成として定義する。（X が n 個の要素からなる有限集合の場合のみを考えても良い。）

解答). $A \ni f, g, h$ に対して, 結合則：$(f \cdot g) \cdot h(x) = (f \cdot g)(h(x)) = f(g(h(x))) = f((g \cdot h)(x)) = f \cdot (g \cdot h)(x)$. 交換則：なし. 例えば, $A = \{1, 2, 3\}$ とし, $f : 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$, $g : 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1$ とする. $f \cdot g : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. $g \cdot f : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$. 単位元：id(恒等写像). 逆元：逆対応.

問題 1.1.2　(1) 前問の 2 項演算について、単位元が存在するものはどれか。存在する場合には、単位元は何かを具体的にあげよ。

(2) 前問の 2 項演算について、どのような A の元には逆元が存在するか。

問題 1.1.3 結合則が成り立つような 2 項演算については有限個の元の積 $x_1 \cdot x_2 \cdots x_n$ はどのように括弧をつけて計算しても結果が等しいことを示せ。

(証明)　元の個数 n と x_n の後ろにある閉じ括弧の個数に関する数学的帰納法を用いて証明する.

(1) 閉じ括弧が 0 個のときは，n に関する数学的帰納法の仮定によりこの命題は正しい.

(2) 閉じ括弧の数が $i(> 0)$ 個のときは，まず初めに一番内側の閉じ括弧に着目しその相方を探す．n に関する数学的帰納法の仮定により，一番内側の括弧の中身についてはどのように括弧をつけても結果は一意的に定まるので，これを a とおく．ここで再び n に関する数学的帰納法の仮定により，残った括弧についても，どのようにつけても結果は一意的である.

以上により，$x_1 \cdot x_2 \cdots x_n$ はどのように括弧をつけて計算しても結果が等しい.　[証明終]

問題 1.1.4 結合則を満足するような 2 項演算について単位元が存在すると仮定すると、その単位元は一意的であることを証明せよ。

(証明)　単位元が 2 つ存在すると仮定し，それらを e，e' とおく．このとき，単位元であることの定義により $e = e\cdot e'$ と $e' = e\cdot e'$ が成り立つので，$e = e'$ が得られる．以上により，単位元が存在すれば一意的に定まる．　[証明終]

問題 1.1.5 結合則を満足し、単位元が存在するような 2 項演算について、x の逆元が存在すると仮定すると、それは x によって一意的に定まることを証明せよ。

(証明)　x の逆元が 2 つ存在すると仮定し，それらを y，z とおく．1 つ前の問題により単位元が存在すれば一意的であるから，それを e と書く．このとき，逆元であることの定義により $x\cdot y = y\cdot x = e$ と $x\cdot z = z\cdot x = e$ が成り立つ．結合律を満たしているので，$y = y\cdot e = y\cdot(x\cdot z) = (y\cdot x)\cdot z = e\cdot z = z$ が得られる．以上により，x の逆元が存在すれば x によって一意的に定まる．　[証明終]

問題 1.1.6 A の元 e について $x\cdot e = x$ が全ての $x\in A$ に対して成立するとき (必ずしも $e\cdot x = x$ は成立しなくてもよい)、この e をこの 2 項演算の右単位元であるという。右単位元は存在するが、単位元は存在しないような 2 項演算の例をあげよ。

(解答)　整数の部分集合 $X = \{0, 1\}$ の中に次のような演算を定義する．$x\cdot y := \max\{0, x-y\}$. このとき，0 は X の右単位元である．$0\cdot 0 = 0$, $0\cdot 1 = 0$, $1\cdot 0 = 1$, $1\cdot 1 = 0$ により X の単位元は存在しない．

問題 1.1.7 単位元 e が存在するような 2 項演算について、$x\in A$ を取ったとき $x\cdot y = e$ が成立するような y を x の右逆元であるという。ある元 x について右逆元は存在するが、それが逆元ではないような 2 項演算の例をあげよ。

(解答)　整数全体からなる集合 $\mathbf{Z}$ の中に次のような演算を定義する．

$$x\cdot y := \begin{cases} x+y-1 & (y<2) \\ xy & (y\geq 2) \end{cases}.$$

このとき，1 は $Y = (\mathbf{Z}, \cdot)$ の単位元である．$2\cdot 0 = 1$, $0\cdot 2 = 0$ により 0 は 2 の右逆元であるが逆元ではない．

1.2　群の定義

- 集合 G 上に結合則を満たす 2 項演算が定義されていて、さらに G が単位元をもち、G の各元が逆元をもつとき、G はこの 2 項演算に関して群をなすという。詳しく言えば、

  (1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $(\forall x, y, z \in G)$

  (2) $\exists e \in G$ such that $x \cdot e = e \cdot x = x$ $(\forall x \in G)$

  (3) $\forall x \in G, \exists x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = e$

- 群 G の任意の 2 元について交換則が成立するとき、この群 G を可換群またはアーベル群であるという。

$$x \cdot y = y \cdot x \quad (\forall x, y \in G)$$

  アーベル群の場合には 2 項演算を $+$ で、単位元を 0 で、x の逆元を $-x$ で表すことも多い。このとき、加法群とも言う。

- 群 G の元の個数が有限個であるとき、G を有限群という。このとき、元の個数を $|G|$ と表し、G の位数という。また、元の個数が無限であるときには無限群という。

- 位数 n の有限群 $G = \{a_1, a_2, \ldots, a_n\}$ においては、各 a_i, a_j $(1 \leqq i, j \leqq n)$ について、$a_i \cdot a_j = a_k$ となる a_k が定まる。これを表にしたものを乗積表という。たとえば位数 2 の群は次の乗積表を持つものに限る。

	e	x
e	e	x
x	x	e

- 同じ乗積表を持つ二つの群は同型であるという。同型な二つの群は区別しない。

- 群 G において、$x^0 = e, x^1 = x, x^2 = x \cdot x, \ldots, x^{n+1} = x^n \cdot x$ と定義する。G にある元 x があって、G の全ての元が x^n という形で表されるとき、この群 G を生成元 x をもつ巡回群であるという。

問題 1.2.1 群 G について次のことが成立することを証明せよ。

(1) $x \cdot y = x \cdot z$ ならば $y = z$
解答). $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot z) \Longrightarrow (x^{-1} \cdot x) \cdot y = (x^{-1} \cdot x) \cdot z \Longrightarrow y = z.$

(2) $x \cdot x = x$ ならば $x = e$
解答). $x^{-1} \cdot (x \cdot x) = (x^{-1} \cdot x) \Longrightarrow (x^{-1} \cdot x) \cdot x = e.$

(3) 任意の $a, b \in G$ に対して $a \cdot x = b$ となる x が一意的に存在する。
解答). 存在: $x = a^{-1} \cdot b$ ととる. 一意性: $a \cdot x = b, a \cdot x^{'} = b \Longrightarrow x = a^{-1} \cdot b = a^{-1} \cdot (a \cdot x^{'}) = (a^{-1} \cdot a) = x^{'}$.

(4) $a \in G$ について、$a \cdot G = \{a \cdot x |\ x \in G\}$、$G \cdot a = \{x \cdot a |\ x \in G\}$ と定義すると、$a \cdot G = G = G \cdot a$ が成立する。
解答). $G \ni \forall b$ に対して, $b = (a \cdot a^{-1}) \cdot b = a \cdot (a^{-1} \cdot b)$. よって, $G \subset a \cdot G$. 逆は, 定義より従う. $G = G \cdot a$ も同様.

(5) $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1}$
解答). 帰納法で示す. $n = 2$ のとき, $(a_2^{-1} \cdot a_1^{-1}) \cdot (a_1 \cdot a_2) = (a_1 \cdot a_2) \cdot (a_2^{-1} \cdot a_1^{-1}) = e$. $n = k - 1$ まで成立と仮定. $(a_1 \cdot a_2 \cdots a_{k-1} \cdot a_k)^{-1} = a_k^{-1} \cdot (a_1 \cdot a_2 \cdots a_{k-1})^{-1} = a_k^{-1} \cdot a_{k-1}^{-1} \cdots a_1^{-1}$.

問題 1.2.2　(1) 位数 $3, 4, 5, 6$ の群の乗積表を書け。これによって、位数 $3, 5$ の群は同型を除いて一通りであること、また位数 $4, 6$ の群は二通りあることを示せ。
解答). $o(G) = 3$ のとき,

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

.

$o(G) = 4$ のとき,

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

,

	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

.

$o(G) = 5$ のとき,

	e	x	y	z	u
e	e	x	y	z	u
x	x	y	z	u	e
y	y	z	u	e	x
z	z	u	e	x	y
u	u	e	x	y	z

.

$o(G) = 6$ のとき,

	e	x	x^2	x^3	x^4	x^5
e	e	x	x^2	x^3	x^4	x^5
x	x	x^2	x^3	x^4	x^5	e
x^2	x^2	x^3	x^4	x^5	e	x
x^3	x^3	x^4	x^5	e	x	x^2
x^4	x^4	x^5	e	x	x^2	x^3
x^5	x^5	e	x	x^2	x^3	x^4

,

	e	x	y	y^2	xy	xy^2
e	e	x	y	y^2	xy	xy^2
x	x	e	xy	xy^2	y	y^2
y	y	xy^2	y^2	e	x	xy
y^2	y^2	xy	e	y	xy^2	x
xy	xy	y^2	xy^2	x	e	y
xy^2	xy^2	y	x	xy	y^2	e

.

(2) 位数 7 の群の乗積表を書くことによって、位数 7 の群は巡回群しかないことを示せ。

解答).

	e	x	x^2	x^3	x^4	x^5	x^6
e	e	x	x^2	x^3	x^4	x^5	x^6
x	x	x^2	x^3	x^4	x^5	x^6	e
x^2	x^2	x^3	x^4	x^5	x^6	e	x
x^3	x^3	x^4	x^5	x^6	e	x	x^2
x^4	x^4	x^5	x^6	e	x	x^2	x^3
x^5	x^5	x^6	e	x	x^2	x^3	x^4
x^6	x^6	e	x	x^2	x^3	x^4	x^5

.

問題 1.2.3 位数 n の巡回群の乗積表を完成せよ。また、これによって位数 n の巡回群は同型を除いて一通りしかないことを示せ。

解答).

	e	x	x^2	$\cdots$	x^{n-1}
e	e	x	x^2	$\cdots$	x^{n-1}
x	x	x^2	x^3	$\cdots$	e
x^2	x^2	x^3	x^4	$\cdots$	x
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x^{n-1}	x^{n-1}	e	x	$\cdots$	x^{n-2}

.

問題 1.2.4 生成元 x を持つ巡回群 G について、次のことを示せ。

(a) G が有限群であるためには $x^n = e$ となる自然数 n が存在することが必要十分である。
解答). ($\Longrightarrow$) $G \ni \forall x$ に対して, $x^n = x^m$, $(n > m)$ となる m が存在する. よって, $x^{n-m} = e$.
($\Longleftarrow$) $\forall k \in \mathbf{Z}$ に対して, $k = qn + r$,$(0 \leq r \leq n)$ とかける. よって, $x^k = x^r$. ゆえに G は有限.

(b) G の位数が n であるとき、n は $x^m = e$ となる最小の自然数 m に等しい。
解答). $x^m = e$ となる m をとる. $\{x, x^2, x^3, \ldots, x^{m-1}, x^m = e\}$ は, すべて異なる元の集合. よって $x^n = e$ より $n = m$.

(c) G の位数が無限であるとき、G は加法群 $\mathbf{Z}$ と同型である。
解答). x を G の生成元とする. $\varphi : G \longrightarrow \mathbf{Z}$, $x^i \longmapsto i$ で定める. $\varphi(x^i x^j) = \varphi(x^{i+j}) = i + j = \varphi(x^i) + \varphi(x^j)$. $\varphi(x^i) = \varphi(x^j) \Longrightarrow i = j \Longrightarrow x^i = x^j$. 全射性は明らか.

問題 1.2.5 次の集合は与えられた 2 項演算に対して群をなすことを確かめよ。また、それぞれの場合に単位元、逆元は何か。

(a) 通常の加法による $\mathbf{Z}$
解答).$Z \ni \forall a, b, c$ に対して, $a+b \in \mathbf{Z}$, $a+(b+c) = a+b+c = (a+b)+c$, 単位元 0, 逆元 $-a$.

(b) 通常の積による $\mathbf{R} - \{0\}$
解答).$\mathbf{R} - \{0\} \ni \forall a, b, c$ に対して, $ab \in \mathbf{R} - \{0\}$, $(ab)c = abc = a(bc)$, 単位元 1, 逆元 $\frac{1}{a}$.

(c) 行列の積による n 次複素正則行列の全体 $GL_n(\mathbf{C})$
解答).$GL_n(\mathbf{C}) \ni A, B, C$ に対して, $\det(AB) = \det A \det B$ より, $AB \in GL_n(\mathbf{C})$, $(AB)C = A(BC)$.
単位元 I_n, 逆元 A^{-1}.

(d) 置換の合成による n 文字の置換の全体 S_n

(解答) 任意の $\sigma, \tau, \rho \in S_n$ に対して, 置換の定義により $(\sigma \cdot \tau) \cdot \rho = \sigma \cdot (\tau \cdot \rho)$ が成り立つので結合律を充たす. 単位元は, 恒等置換 ε であり, $\sigma \in S_n$ の逆元は σ の逆置換である.

(e) 集合 M からそれ自身への全単射の全体 G に写像の合成で演算を入れる。

(解答) 任意の $f, g, h \in G$ に対して, $(f \circ g) \circ h = f \circ (g \circ h)$ により結合律を充たす. 単位元は, 恒等写像 1_M であり, $f \in G$ の逆元は f の逆写像である.

問題 1.2.6 群 G が位数 n の有限群であるとき、任意の元 $x \in G$ に対して、$x^m = e$ となる n 以下の自然数 m が存在することを証明せよ。

(証明) 任意の $x \in G$ に対して, 部分群 $\langle x \rangle \subset G$ の位数は n 以下である. よって, $x^m = e$ を充たす n 以下の自然数が存在する. [証明終]

問題 1.2.7 次の文章の下線部の内容が正しいことを証明せよ。
「与えられた $n \in \mathbf{Z}$ について、整数 x, y は、$x - y$ が n で割り切れるとき、n を法として合同であるといい、

$$a \equiv b \mod n$$

とかく。この 合同という関係は同値関係 なので、それによって $\mathbf{Z}$ を類別することができ、その同値類の集合を $\mathbf{Z}/n\mathbf{Z}$ を書く。整数 x と合同な整数の集合を $[x]$ と表すと、

$$\mathbf{Z}/n\mathbf{Z} = \{[0], [1], [2], \ldots, [n-1]\}$$

となることが分かる。この $\mathbf{Z}/n\mathbf{Z}$ 上に加法的な 2 項演算 $[x] + [y]$ を $[x + y]$ と与えるとこれは矛盾なく定義されて、これによって $\mathbf{Z}/n\mathbf{Z}$ はアーベル群となる。このアーベル群の単位元は $[0]$ である。また、$\mathbf{Z}/n\mathbf{Z}$ は 元 $[1]$ によって生成される位数 n の巡回群である。
位数 n の任意の巡回群はこの $\mathbf{Z}/n\mathbf{Z}$ に同型である。」

解答).(i).$x \equiv y \Longleftrightarrow n|x-y$ とする. $x-x=0$ より, $n|0$. よって, $x \equiv x$. 同様に, $x \equiv y$, $y \equiv x \Longrightarrow x \equiv x$. $x \equiv y, y \equiv z \Longrightarrow x \equiv z$.
(ii).$[x] \ni x_1, [y] \ni y_1$ に対して, $x_1 + x_2 \in [x+y]$ を示せばよい. $x_1 = x + nk,\ y_1 = y + nk^{'} \Longrightarrow x_1 + y_1 = (x+y) + n(k+k^{'})$.
(iii),(iv).$([x]+[y])+[z] = [x+y]+[z] = [x+y+z] = [x]+[y+z] = [x]+([y]+[z])$. $[x]+[y] = [x+y] = [y+x] = [y]+[x]$. $[x]+[0] = [x+0] = [0+x] = [0]+[x] = [x]$. よって, 単位元 $[0]$. $[x]+[-x] = [x-x] = [0] = [-x+x] = [-x]+[x]$. よって, 逆元 $[-x]$.
(v),(vi). G の生成元を x とする. $\varphi : G \longrightarrow \mathbf{Z}/n\mathbf{Z}$ 準同型, $x \longmapsto [1]$ とする. $\varphi(x^i) = \varphi(x^j) \Longrightarrow [i] = [j] \Longrightarrow x^i = x^j$. 全射は明らか. よって, $G \cong \mathbf{Z}/n\mathbf{Z}$ ゆえに (iv) は, 成立.

1.3　部分群による剰余類、ラグランジュの定理

- 群 G の空でない部分集合 H が G と同じ演算で群になっているとき、H は G の部分群であるという。
- G の部分集合 H が G の部分であるための必要十分条件は、G の単位元 e について $e \in H$ であり、かつ、$x, y \in H \Rightarrow x \cdot y^{-1} \in H$ となることである。
- H が G の部分群であるとき、G の 2 元 x, y に対して、$x \sim y$ を $x^{-1} \cdot y \in H$ と定義することで、同値関係 $\sim$ が得られる。この同値関係による同値類の集合を G/H と書く。

  $aH = \{ah \mid h \in H\}$ とおいて、G/H は集合として、$\{aH|\ a \in G\}$ である。各 aH を a の H に関する左剰余類という。$x \sim y \Leftrightarrow xH = yH$ である。
- 上と同様に、G の 2 元 x, y に対して、$x \sim' y$ を $x \cdot y^{-1} \in H$ と定義することで、同値関係 $\sim'$ が得られる。この同値関係による同値類の集合を $H\backslash G$ と書く。

  $Ha = \{ha \mid h \in H\}$ とおいて、$H\backslash G$ は集合として、$\{Ha|\ a \in G\}$ である。各 Ha を a の H に関する右剰余類という。$x \sim' y \Leftrightarrow Hx = Hy$ である。
- 集合としての G/H の濃度を部分群 H の指数といい、$[G : H]$ と書く。
- (ラグランジュの定理)　$|G| = |H| \cdot [G : H]$
- G が有限群のとき、その部分群 H の位数 $|H|$ と指数 $[G : H]$ は $|G|$ の約数である。
- 群 G の任意の元 x について、$x^n = e$ となる最小の自然数 n を元 x の位数 (order) といって $ord(x)$ という記号で表す。ラグランジュの定理より、G が有限群のとき $ord(x)$ はいつも $|G|$ の約数である。

問題 1.3.1 次のそれぞれの場合に群 G の部分集合 H が部分群になっていることを確認せよ。

(a) $G = \mathbf{R}$ （加法群）の部分集合 $H = \mathbf{Z}$

(b) 任意の群 G とその元 x について部分集合 H を $H = \{x^n|\ n \in \mathbf{Z}\}$ と定義する。

(c) $G = GL(n, \mathbf{C}) = \{X|\ n$ 次複素行列で $\det(X) \neq 0\}$ の部分集合 $H = SL(n, \mathbf{C}) = \{X \in GL(n, \mathbf{C})|\ \det(X) = 1\}$

(d) $G = GL(n, \mathbf{C}) = \{X|\ n$ 次複素行列で $\det(X) \neq 0\}$ の部分集合 $T = \{X \in GL(n, \mathbf{C})|\ X$ は上三角行列 $\}$

(e) $G = SL(2, \mathbf{R})$ の部分集合 $H = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mid t \neq 0 \in \mathbf{R} \right\}$

(f) n 文字の置換全体（対称群）$G = S_n$ における偶置換の全体 $H = A_n$

(証明)　(a) (1) G の単位元 0 は H に属する．(2) 任意の $m, n \in H$ に対して，$m + (-n) = m - n \in H$ を充たす．以上により，H は G の部分群である．

(b) (1) G の単位元 $1 = x^0$ は H に属する．(2) 任意の $x^m, x^n \in H$ に対して，$x^m \cdot x^{-n} = x^{m-n} \in H$ を充たす．以上により，H は G の部分群である．

(c) (1) G の単位元 E(単位行列) は H に属する．(2) 任意の $A, B \in H$ に対して，det の計算をすることにより $AB^{-1} \in H$ を充たすことが分かる．以上により，H は G の部分群である．

(d) (1) G の単位元 E(単位行列) は H に属する．(2) 任意の $A, B \in H$ に対して，余因子行列を計算することにより $AB^{-1} \in H$ を充たすことが分かる．以上により，H は G の部分群である．

(e) (1) G の単位元 E(単位行列) は H に属する．(2) 任意の $A, B \in H$ に対して，簡単な計算により $AB^{-1} \in H$ を充たすことが分かる．以上により，H は G の部分群である．

(f) (1) G の単位元 ε(恒等置換) は H に属する．(2) 任意の $\sigma, \tau \in H$ に対して，偶置換の逆元もまた偶置換であることから $\sigma\tau^{-1} \in H$ を充たすことが分かる．以上により，H は G の部分群である．

[証明終]

問題 1.3.2 全問の各 G と H について、その左剰余類の集合 G/H と右剰余類の集合 $H\backslash G$ の集合を求めよ。

(解答)　(a) G/H は集合として，$\{r + H | r \in G\}$ である．$r + H = r' + H \iff r - r' \in H$ により，$G/H \cong [0, 1) \cong S^1$ が得られる．(ただし，$\cong$ は集合としての一対一対応を表わすものとする．群構造云々はひとまず無視する．)

$H\backslash G$ は集合として，$\{H+r | r \in G\}$ である．$H+r = H+r' \iff r-r' \in H$ により，$H\backslash G \cong [0, 1) \cong S^1$ が得られる．

(b) G/H は集合として，$\{gH | g \in G\}$ である．ただし, $gH = g'H \iff g'^{-1}g \in H$.

$H \setminus G$ は集合として，$\{Hg | g \in G\}$ である．ただし, $Hg = Hg' \iff g'g^{-1} \in H$.

(c) G/H は集合として，$\{AH | A \in G\}$ である．$AH = BH \iff B^{-1}A \in H$ により，$G/H \cong \mathbf{C}^\times$ が得られる．

$H \setminus G$ は集合として，$\{HA | A \in G\}$ である．$HA = HB \iff AB^{-1} \in H$ により，$H \setminus G \cong \mathbf{C}^\times$ が得られる．

(d) G/H は集合として，$\{AH | A \in G\}$ である．ただし, $AH = BH \iff B^{-1}A \in H$.

$H \setminus G$ は集合として，$\{HA | A \in G\}$ である．ただし, $HA = HB \iff AB^{-1} \in H$.

(e) G/H は集合として，$\{AH | A \in G\}$ である．ただし, $AH = BH \iff B^{-1}A \in H$.

$H \setminus G$ は集合として，$\{HA | A \in G\}$ である．ただし, $HA = HB \iff AB^{-1} \in H$.

(f) G/H は集合として，$\{\sigma H | \sigma \in G\}$ である．$\sigma H = \tau H \iff \tau^{-1}\sigma \in H$ により，$G/H \cong \langle -1 \rangle \cong \mathbf{Z}/2\mathbf{Z}$ が得られる．

$H \setminus G$ は集合として，$\{H\sigma | \sigma \in G\}$ である．$H\sigma = H\tau \iff \sigma\tau^{-1} \in H$ により，$H \setminus G \cong \langle -1 \rangle \cong \mathbf{Z}/2\mathbf{Z}$ が得られる．

問題 1.3.3 $n = pq$ （ただし p, q は互いに素な素数）のとき、アーベル群 $G = \mathbf{Z}/n\mathbf{Z}$ の全ての部分群をもとめよ。

(解答) G の非自明な部分群 H の元 x の位数は $n = pq$ の約数であるから, p または q である. x の位数が p のとき, $\{0\} \neq H_p := \{0, x, 2x, \ldots, (p-1)x\} \subset H$ であり, 指数を比べることにより $H_p = H$ を得る. x の位数が q のときも同様である. 以上により, G の部分群は G,H_p,H_q,$\{0\}$ の 4 種類である.

問題 1.3.4 G が位数 n の有限群であるとき、もし G に位数 n の元 x が存在すれば、G は x を生成元にもつ巡回群であることを証明せよ。

(証明) 仮定により, 任意の $1 \leq m < n$ に対して, $x^m \neq e$ かつ $x^n = e$ が成り立つので, 任意の $1 \leq \ell < k \leq m$ に対して, $x^\ell \neq x^k$ を充たす. 故に, G は x を生成元にもつ巡回群である. [証明終]

問題 1.3.5 G が巡回群であるとき、G の任意の部分群はまた巡回群であることを証明せよ。

(証明) G の生成元を x とおき, $G = \langle x \rangle$ と書く. G の任意の部分群 $H(\neq G)$ に対して, $y \in H$ ならば $y \in G = \langle x \rangle$ により, ある整数 n を選ぶと $y = x^n$ を充たす. 正の整数 n の中で, $x^n \in H$ を充たすものの最小のものを r とおくとき, $\langle x^r \rangle \subset H \subsetneq G$ であるから, $H \subset \langle x^r \rangle$ であることを証明すればよい. $x^n \in H$ を充たす全ての整数 n に対して, $n = mr + \ell$, 但し $0 \leq \ell \leq r-1$ と表わす. このとき, $x^n = x^{mr+\ell} = x^{mr}x^\ell \in H$ により, $x^\ell \in H$ を充たす. よって, $\ell = 0$ となるので, $H = \langle x^r \rangle$ を充たす. すなわち, H は巡回群である. [証明終]

問題 1.3.6 G が位数 n の有限巡回群であるとき、n の任意の約数 m に対して、位数 m の G の部分群がただ一つだけ存在することを証明せよ。

解答).$G := \{x, x^2, x^3, \ldots, x^{n-1}, x^n = e\}$. $n = md$ とすると, $H := \{x^d, x^{2d}, \ldots, x^{(m-1)d}, x^{(md)} = e\}$ ととればよい. K を位数 m の群とする.$K \ni y$ に対して, $y^m = e$. i.e. $y \in H$. よって $K = H$.

問題 1.3.7 G が有限群で H がその部分群であるとき、G/H の元の個数と $H\backslash G$ の元の個数は等しいことを示せ。

(証明) 対応 $\varphi : G/H \to H \setminus G$ を $gH \mapsto Hg$ で与える. $g_2^{-1}g_1 \in H$ ならば, $g_1^{-1}g_2 = (g_2^{-1}g_1)^{-1} \in H$ であるから, φ は $well\text{-}defined$ な写像を成す. φ の全射性は明らかである. 群の定義により φ の単射性も簡単に導かれる. 以上により, G/H の元の個数と $H \setminus G$ の元の個数は等しい. [証明終]

問題 1.3.8 加法群 $\mathbf{Q}$ は指数有限の部分群を持たないことを証明せよ。

解答).H は, $\mathbf{Q}$ と異なる部分群とする. $\mathbf{Q} \triangleright H$, $[\mathbf{Q} : H] = n < \infty$. と仮定する. $\forall y \in \mathbf{Q}/H$ に対して, $\mathbf{Q}/H$ は群となるので, $ny = 0$. $\forall x \in \mathbf{Q}$ に対して, $\exists z \in \mathbf{Q}$, s.t. $x = nz$. また, $\forall x \in \mathbf{Q}$ に対して, $nx \in H$ であった. よって, $nz = x \in H$. これは仮定に矛盾.

問題 1.3.9 有限群 G とその部分群 H に加えて、H の部分群 K があるとき、等式 $[G : K] = [G : H][H : K]$ が成立することを証明せよ。

解答). ラグランジュの定理より $[G : K] = o(G)/o(K) = o(G)/o(H) \times o(H)/o(K) = [G : H][H : K]$.

問題 1.3.10 一般に群 G はその生成元（無限個かもしれない）とそれらの間の関係式で一意的に定めることができる。たとえば、$G = \langle x \rangle / (x^n = e)$ と書くと、G の任意の元は x^i という形で表されて x^n は単位元 e になることを意味するので、この G は x を生成元に持つ位数 n の巡回群である。次の様にして生成元と関係式で表される群について、その位数は何か？　また、それぞれの場合において部分群を全て決定せよ。

(a) $G = \langle x \rangle$ （関係式なし）

(b) $G = \langle x, y \rangle / (x^2 = e, y^2 = e, xy = yx)$

(c) $G = \langle x, y \rangle / (x^3 = e, y^2 = e, yx = x^2 y)$

(証明)　(a) 対応 $\varphi : \mathbf{Z} \to G = \langle x \rangle$ を $n \mapsto x^n$ で与えると, *well-defined* な写像を成す. 関係式がないことから, φ は同型写像である. よって, G の位数は無限であり, G の部分群は $H_i = \langle x^i \rangle$ $(i = 0, 1, 2, \ldots)$ の型で表わせる.

(b) $G = \langle x, y \rangle / (x^2 = e, y^2 = e, xy = yx) = \{e, x, y, xy\} (\cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z})$ により, G の位数は 4 であり, G の部分群は G,$\{e, x\}$,$\{e, y\}$,$\{e, xy\}$,$\{e\}$ の 5 種類である.

(c) $G = \langle x, y \rangle / (x^3 = e, y^2 = e, yx = x^2 y) = \{e, x, x^2, y, xy, x^2 y\} (\cong S_3)$ により, G の位数は 6 であり, G の部分群は G,$\{e, x, x^2\}$,$\{e, y\}$,$\{e, xy\}$,$\{e, x^2 y\}$,$\{e\}$ の 6 種類である.

[証明終]

問題 1.3.11 （オイラー関数）　自然数 n に対して、巡回群 $\mathbf{Z}/n\mathbf{Z}$ における位数 n の元の個数を $\varphi(n)$ と表し、φ をオイラー関数という。

(a) $\varphi(n)$ は集合 $\{i \mid 1 \leqq i < n,\ (i, n) = 1\}$ の元の個数に等しいことを示せ。
解答). $i \in \mathbf{Z}/n\mathbf{Z}$ に対して, $gcd(n, i) = 1 \Longleftrightarrow i$ は, $\mathbf{Z}/n\mathbf{Z}$ の生成元. を示せばよい.
$(\Longrightarrow)$ $k_1 n + k_2 i = 1, \exists k_1, k_2 \in \mathbf{Z}$, $k_2 s \equiv 1 \pmod{\text{n}}$ よって, $< s > \ni 1$.
$(\Longleftarrow)$ 上を逆にたどればよい.

(b) p が素数のとき $\varphi(p^r) = p^{r-1}(p - 1)$ となることを示せ。
解答).p^r と互いに素な p^r までの自然数を数え上げればよい.

(c) 等式 $n = \sum_{m \text{ は } n \text{ の約数}} \varphi(m)$ を証明せよ。

解答). $n = p_1^{i_1} p_2^{i_2} \cdots p_t^{i_t}$, $m = p_1^{j_1} p_2^{j_2} \cdots p_t^{j_t}$, $j_1 \leq i_1, j_2 \leq i_2, \ldots, j_t \leq i_t$ とする.
$n = p_1^{i_1} p_2^{i_2} \cdots p_t^{i_t} = \sum_{(j_1, j_2, \ldots, j_t) \leq (i_1, i_2, \ldots, i_t)} \varphi(p_1^{j_1} p_2^{j_2} \cdots p_t^{j_t})$ と書き換えられる. $gcd(n, m) = 1$ のとき,

$\varphi(nm)=\varphi(n)\varphi(m)$ となることに注意すれば,

$$
\begin{aligned}
\text{右辺} &= \sum_{(j_1,j_2,\dots,j_t)\le(i_1,i_2,\dots,i_t)} \varphi(p_1^{j_1})\varphi(p_2^{j_2})\cdots\varphi(p_t^{j_t}) \\
&= \sum_{(j_1,j_2,\dots,j_t)\le(i_1,i_2,\dots,i_t)} (p_1^{j_1}-p_1^{j_1-1})(p_2^{j_2}-p_2^{j_2-1})\cdots(p_t^{j_t}-p_t^{j_t-1}) \\
&= \sum_{(j_1,j_2,\dots,j_t-1)\le(i_1,i_2,\dots,i_t-1)} (p_1^{j_1}-p_1^{j_1-1})(p_2^{j_2}-p_2^{j_2-1})\cdots(p_{t-1}^{j_{t-1}}-p_{t-1}^{j_{t-1}-1})\sum_{j_t\le i_1} p_t^{j_t}-p_t^{j_t-1} \\
&= \sum_{(j_1,j_2,\dots,j_t-1)\le(i_1,i_2,\dots,i_t-1)} (p_1^{j_1}-p_1^{j_1-1})(p_2^{j_2}-p_2^{j_2-1})\cdots(p_{t-1}^{j_{t-1}}-p_{t-1}^{j_{t-1}-1})p_t^{i_t} \\
&= p_1^{i_1}p_2^{i_2}\cdots p_t^{i_t}.
\end{aligned}
$$

1.4　準同型写像

- 二つの群 G と G' の間の写像 $f : G \to G'$ について、f が次の条件を満たすとき f を（群の）準同型写像であるという。

  (a) 任意の $x, y \in G$ について $f(x \cdot y) = f(x) \cdot f(y)$ （積を積に写す）

- f が準同型であるならば、次のことが成立する。

  (b) $f(e) = e'$ （単位元を単位元に写す）

  (c) $f(x^{-1}) = f(x)^{-1}$ （逆元を逆元に写す）

  (d) $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1}$

  言い換えれば、準同型とは群の演算構造を保つような写像である。

- 準同型 $f : G \to G'$ が全単射であるとき、f を同型写像であるといい、同型写像がその間に存在するような二つの群 G と G' は同型であるという。このとき、$G \cong G'$ と表す。

- 準同型 $f : G \to G'$ に対して、

$$\mathrm{Im}(f) = \{f(x) \in G' |\ x \in G\}$$

  と定義し、この $\mathrm{Im}(f)$ を準同型写像 f の像 (Image) という。$\mathrm{Im}(f)$ はいつも群 G' の部分群である。準同型 $f : G \to G'$ に対して、この f が全射であるための必要十分条件は、$\mathrm{Im}(f) = G'$ となることである。

- 準同型 $f : G \to G'$ に対して、

$$\mathrm{Ker}(f) = \{x \in G |\ f(x) = e'\}$$

  と定義し、この $\mathrm{Ker}(f)$ を準同型写像 f の核 (Kernel) という。$\mathrm{Ker}(f)$ はいつも群 G の部分群である。準同型 $f : G \to G'$ に対して、この f が単射であるための必要十分条件は、$\mathrm{Ker}(f) = \{e\}$ となることである。

問題 1.4.1 f が準同型であるならば、f は単位元を単位元に写すこと、逆元を逆元に写すこと、$f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1}$ となることを証明せよ。

解答).$f(e) = f(ee) = f(e)f(e)$. よって, $e = f(e)$. $f(e) = f(xx^{-1}) = f(x)f(x^{-1})$. よって, $f(x)^{-1} = f(x^{-1})$. $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1}$.

問題 1.4.2 次の群の間の写像が準同型写像であることを確かめよ。

(a) $f : GL(n, \mathbf{C}) \to GL(1, \mathbf{C})$ を $f(A) = det(A)$ と与える。
解答). $GL(n, \mathbf{C}) \ni A, B$ に対して, $f(AB) = det(AB) = det(A)det(B) = f(A)f(B)$.

(b) 加法群 $\mathbf{R}$ と乗法群 $\mathbf{C}^\times = \mathbf{C} - \{0\} = GL(1, \mathbf{C})$ に対して、$f : \mathbf{R} \to \mathbf{C}^\times$ を $f(x) = e^{2\pi ix}$ と定義する。
解答). $\mathbf{R} \ni \forall x, y$ に対して, $f(x + y) = e^{2\pi i(x+y)} = e^{2\pi ix}e^{2\pi iy} = f(x)f(y)$.
$\mathrm{Ker}(f) = \{x \in \mathbf{R} |\ e^{2\pi ix} = 1\}$, $e^{2\pi ix} = cos2\pi x + isin2\pi x$. なので, $\mathrm{Ker}(f) = Z$.

(c) $f : \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ を

$$f(x) = \begin{cases} 0 & (x \text{ が偶数のとき}) \\ 1 & (x \text{ が奇数のとき}) \end{cases}$$

と定義する。解答).

$$f(x+y) = \begin{cases} 0 & (x, y \text{ がどちらも偶数か奇数のとき}) \\ 1 & (\text{それ以外}) \end{cases},$$

$$f(x) = \begin{cases} 0 & (x \text{ が偶数のとき}) \\ 1 & (x \text{ が奇数のとき}) \end{cases},$$

$$f(y) = \begin{cases} 0 & (y \text{ が偶数のとき}) \\ 1 & (y \text{ が奇数のとき}) \end{cases},$$

$$f(x)+f(y) = \begin{cases} 0 & (x, y \text{ がどちらも偶数か奇数のとき}) \\ 1 & (\text{それ以外}) \end{cases}$$

$\mathrm{Ker}(f) = 2Z$.

(d) n 文字の置換の全体 S_n （n 次対称群）に対して、$f : S_n \to \mathbf{Z}/2\mathbf{Z}$ を $f(\sigma) = sgn(\sigma)$ と定義する。ただし、$sgn(\sigma)$ は置換 σ の符号を表し、

$$sgn(\sigma) = \begin{cases} 0 & (x \text{ が偶置換のとき}) \\ 1 & (x \text{ が奇置換のとき}) \end{cases}$$

と定義される。

(証明) (奇置換) · (奇置換) = (偶置換), (奇置換) · (偶置換) = (奇置換), (偶置換) · (奇置換) = (偶置換), (偶置換) · (偶置換) = (偶置換) であり f で写すと, それぞれ $1+1=0$, $1+0=1$, $0+1=1$, $0+0=0$ を充たしているので, f は準同型写像である. また, $\mathrm{Ker}(f) = \{$ 偶置換 $\} = A_n$ である. [証明終]

問題 1.4.3 全問の各準同型写像に対して、その核を求めよ。

問題 1.4.4 準同型写像 $f : G \to G'$ に対して次のことを証明せよ。

(a) f が単射で G' がアーベル群ならば G もアーベル群。
解答).$G \ni \forall x, y$ に対して, $f(xy) = f(x)f(y) = f(y)f(x) = f(yx)$. f の単射性より, $xy = yx$.

(b) f が全射で G がアーベル群ならば G' もアーベル群。
解答).$G' \ni x, y$ に対して, $x = f(a)$, $y = f(b)$ とする. $xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$.

問題 1.4.5 G と G' が有限群で、同型写像 $f : G \to G'$ があるとき、この f による対応で G の乗積表と G' の乗積表は同じものになることを確かめよ。したがって、乗積表を使って以前に与えた同型の定義とこの節での同型の定義は一致する。

解答).G の乗積表と G' の乗積表が等しい必要十分条件は G での演算が G' での演算を保つことである．これは同型写像 $f : G \to G'$ があることに他ならない.

問題 1.4.6 同型写像 $f : G \to G'$ があるとき、その逆写像 $f^{-1} : G' \to G$ もまた群の同型写像になることを証明せよ。

解答).$G' \ni \forall a$ に対して, $f(a) = a'$ とする．$f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b')$.
$f^{-1}(a') = f^{-1}(b') \Longrightarrow a = b \Longrightarrow f(a) = f(b) \Longrightarrow a' = b'$．全射性は, 明らか.

問題 1.4.7 準同型 $f : G \to G'$ について、

(a) f が単射であるための必要十分条件は、$\mathrm{Ker}(f) = \{e\}$ であることを証明せよ。

(b) $\mathrm{Ker}(f) = \{e\}$ であるならば、G は群 $\mathrm{Im}(f)$ と同型であることを証明せよ。

(証明) (a) f が単射であると仮定すると, f が準同型写像であることから $\mathrm{Ker}(f) = \{e\}$ が得られる．逆に $\mathrm{Ker}(f) = \{e\}$ であるとき $f(x) = f(y)$ と仮定すると, $e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ により, $xy^{-1} = e$ が得られる．すなわち, $x = y$ を充たす．故に, f は単射である．
(b) 準同型 $f : G \to \mathrm{Im}(f)$ の全射性は明らかである．仮定により f は単射でもあるので, f は同型写像である．　[証明終]

問題 1.4.8 群 G からそれ自身への写像 $f : G \to G$ を $f(x) = x^{-1}$ と定義する。この f はいつでも全単射であることを示せ。次に、f が準同型写像であるためには、群 G がアーベル群であることが必要十分であることを示せ。

(証明) 任意の $x \in G$ に対して, $x^{-1} \in G$ を選ぶと, $f(x^{-1}) = (x^{-1})^{-1} = x$ を充たすので, f は全射である．$f(x) = f(y)$ と仮定するとき, $x^{-1} = y^{-1}$ により $x = y$ が成り立つので, f は単射である．以上により f は全単射である．ここで f が準同型写像であると仮定すると, $f(xy) = f(x)f(y)$ により, $(xy)^{-1} = x^{-1}y^{-1}$ が成り立つ．両辺に左から xy 右から yx をかけることにより, $yx = xy$ が得られるので G はアーベル群である．逆に G がアーベル群であると仮定すると, 任意の $x, y \in G$ に対して, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$ が成り立つので, f は準同型写像である．　[証明終]

問題 1.4.9 群 G からそれ自身への写像 $f : G \to G$ を $f(x) = x^2$ と定義するとき、これが準同型写像であるためには、群 G がアーベル群であることが必要十分であることを示せ。

解答).($\Longrightarrow$) $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$ より, $(xy)(xy) = x^2y^2$ よって, $yx = xy$.
($\Longleftarrow$) $f(xy) = (xy)^2 = xyxy = x^2y^2 = f(x)f(y)$.

問題 1.4.10 加法群 $\mathbf{Q}$ からそれ自身への準同型写像 $f : \mathbf{Q} \to \mathbf{Q}$ について、$f(1) = 1$ が満たされるならば、f は恒等写像であることを示せ。

解答).$Q \ni a,\ b,\ gcd(a, b) = 1$ とする．$1 = f(1) = f(b(1/b)) = bf(1/b)$, より $f(a/b) = af(1/b) = a/b$.

問題 1.4.11 加法群 $\mathbf{Z}$ と加法群 $\mathbf{Q}$ は群として同型ではないことを証明せよ。

解答). もし同型ならば，ある有理数 $q \in \mathbf{Q}$ があって，すべての有理数はこの q の整数倍でなくてはならない。しかし，$q/2$ は q の整数倍にはならない。

問題 1.4.12 正の有理数の全体 $\mathbf{Q}^+ = \{x \in \mathbf{Q} |\ x > 0\}$ は乗法に関して群となる。この乗法群 $\mathbf{Q}^+$ は加法群 $\mathbf{Z}$ とも $\mathbf{Q}$ とも同型にはなりえないことを証明せよ。

解答).$(\mathbf{Q}^+, \times) \not\simeq (\mathbf{Z}, +)$ を示す. $f : \mathbf{Z} \to \mathbf{Q}^+$ 同型写像 があるとする. $f(1) = a$ とすると $f(i) = a^i, i \in \mathbf{Z}$ となる. これは, 明らかに全射でない. よって f の全射性に矛盾. 同様に, $(\mathbf{Q}^+, \times) \not\simeq (\mathbf{Q}, +)$ を示す. $f : \mathbf{Q} \to \mathbf{Q}^+$ 同型写像 があるとする. ここで, $f(a) = 2$ とすると $f(a/2) = \pm\sqrt{2}$ でなくてはならない。 これは矛盾。

問題 1.4.13 群 G とその固定した元 $a \in G$ について、写像 $\phi_a : G \to G$ を $\phi_a(x) = axa^{-1}$ と定義する。この ϕ_a はいつでも群 G の同型写像となることを証明せよ。この ϕ_a を a による群 G の内部自己同型という。

解答). (準同型): $\phi_a(xy) = axa^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_b(y)$. (単射): $\phi_a(x) = \phi_b(y) \Longrightarrow axa^{-1} = aya^{-1} \Longrightarrow x = y$. (全射): $\phi_a(a^{-1}xa) = x$.

1.5　正規部分群と剰余群

- 群 G の部分群 N が次の同値な条件のどれかを満たすときに N を G の正規部分群 (normal subgroup) であるという。

  (a) $xN = Nx \quad$ for any $x \in G$

  (b) $xNx^{-1} = N \quad$ for any $x \in G$

  (c) $xNx^{-1} \subseteqq N \quad$ for any $x \in G$

- N が G の正規部分群であるときには、G の任意の部分群 H について、$NH = HN$ が成立する。

- G がアーベル群ならば、G の全ての部分群は正規部分群である。

- $f : G \to G'$ が群の準同型写像であるとき、$\mathrm{Ker}(f)$ はいつでも G の正規部分群である。$\mathrm{Im}(f)$ は必ずしも G' の正規部分群ではないことに注意。

- N が G の正規部分群であるときには、剰余類の集合 G/N に自然に群構造が定義される。この群 G/N を G の N による剰余群という。G/N における積の定義の仕方は、二つのクラス xN と yN に対して、その積を xyN によって与えることによって得られる。これが well-defind であることは、

$$xN = x'N,\ yN = y'N \qquad \Rightarrow\ xyN = x'y'N$$

  を確かめることになるが、これはほとんど N が正規部分群であることの定義と同じである。

  G/N の単位元は $N = eN$, xN の逆元は $x^{-1}N$ で与えられる。

問題 1.5.1 群 $GL(2, \mathbf{R})$ の次の部分群は正規部分群であるか？

(a) $N_1 = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \middle| \ ab \neq 0,\ c \in \mathbf{R} \right\}$

解答).

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \notin N_1.$$

(b) $N_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \ ab \neq 0 \right\}$

解答).

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix} \notin N_2.$$

(c) $N_3 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \ a \neq 0, b \in \mathbf{R} \right\}$

解答).

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \notin N_3.$$

(d) $N_4 = \left\{ \left(\begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) \middle| \ b \in \mathbf{R} \right\}$

解答).

$$\left(\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \cdot \left(\begin{array}{cc} 1 & 0 \\ -1 & 1 \end{array} \right) = \left(\begin{array}{cc} 0 & 1 \\ -1 & 2 \end{array} \right) \notin N_4.$$

問題 1.5.2 H が G の指数 2 の部分群ならば H は G の正規部分群である。このことを証明せよ。

(証明) 任意の $g \in G$ に対して, $g \in H$ のとき $gHg^{-1} \subset H$ であることは明らかである. $g \notin H$ のとき, $gH \neq H \neq Hg$, $H \cap gH = \emptyset = H \cap Hg$ および $H \cup gH = G = H \cup Hg$ が成り立つ. よって, $gH = Hg$ すなわち $gHg^{-1} = H$ が成り立つ. 故に, H は正規部分群である. [証明終]

問題 1.5.3 N と H がともに G の正規部分群で、$N \cap H = \{e\}$ が成り立つとき、N の元と H の元は互いに可換であることを証明せよ。

(証明) 任意の $x \in N$ と任意の $y \in H$ に対して, 正規部分群の定義により $xyx^{-1} \in H$ と $yx^{-1}y^{-1} \in N$ を充たす. よって, $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in N \cap H = \{e\}$ により, $xy = yx$ が成り立つ. [証明終]

問題 1.5.4 G の n 個の正規部分群 H_i $(i = 1, 2, \ldots, n)$ があるとき、それらの共通部分 $N = \cap_{i=1}^{n} H_i$ もまた G の正規部分群であることを証明せよ。

解答).$N \ni \forall a, b$ に対して, $ab^{-1} \in H_i, (i = 1, 2, \ldots, n)$. $N \ni \forall a$,$G \ni \forall x$ に対して, $xax^{-1} \in H_i, (i = 1, 2, \ldots, n)$.

問題 1.5.5 N が G の正規部分群、H が G の部分群であるときに、次のことを証明せよ。

(a) $H \cap N$ は H の正規部分群である。

(b) $NH = \{n \cdot h \mid n \in N,\ h \in H\}$ は G の部分群である。

(c) さらに H も G の正規部分群であるときには、NH は G の正規部分群となる。

(証明) (a) 任意の $x \in H \cap N$ と任意の $h \in H$ に対して, N は G の正規部分群であるので, $hxh^{-1} \in N$ を充たす. また H は G の部分群であるので, $hxh^{-1} \in H$ を充たす. よって, $hxh^{-1} \in H \cap N$ を充たすので, $H \cap N$ は H の正規部分群である.
(b) 任意の $n_1, n_2 \in N$ と任意の $h_1, h_2 \in H$ に対して, $(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 \in NH$ を充たす. $e = e \cdot e \in NH$ を選ぶと, 任意の $nh \in NH$ に対して, $e(nh) = nh = (nh)e$ を充たす. 任意の $nh \in NH$ に対して, $h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH$ を選ぶと, $(nh)(h^{-1}n^{-1}) = e = (h^{-1}n^{-1})(nh)$ を充たす. よって, NH は G の部分群である.
(c) 任意の $nh \in NH$ と任意の $g \in G$ に対して, $g(nh)g^{-1} = (gng^{-1})(ghg^{-1}) \in NH$ を充たす. よって, NH は G の正規部分群である. [証明終]

問題 1.5.6 4 次の対称群 S_4 の全ての部分群を求めて、そのうちどれが正規部分群であるかを指摘せよ。

(解答)　S_4 の部分群 H の位数を n とおくとき, n は 24 の約数のうちのいずれかである.
$\cdot n = 1$ のとき, $H = \{\varepsilon\}$ であり, 正規部分群である.
$\cdot n = 2$ のとき, H は $\mathbf{Z}/2\mathbf{Z}$ と同型な部分群であり 9 種類存在する. いずれの H も S_4 の正規部分群でない.
$\cdot n = 3$ のとき, H は 3-シロー部分群であり 4 種類存在する. いずれの H も S_4 の正規部分群でない.
$\cdot n = 4$ のとき, H は 4 次の巡回群が 3 種類または, $\{\varepsilon, (1,2), (3,4), (1,2)(3,4)\}$ の型の群が 3 種類存在する. これらの場合は, いずれの H も S_4 の正規部分群でない. 特別な場合として, クラインの 4 元群 $V = \{\varepsilon, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ があり, これは正規である.
$\cdot n = 6$ のとき, H は S_3 と同型な部分群であり 4 種類存在する. いずれの H も S_4 の正規部分群でない.
$\cdot n = 8$ のとき, H は 2-シロー部分群であり 3 種類存在する. いずれの H も S_4 の正規部分群でない.
$\cdot n = 12$ のとき, $H = A_4$ であり, 正規部分群である.
$\cdot n = 24$ のとき, $H = S_4$ であり, 正規部分群である.

問題 1.5.7 一般に n 次の対称群 S_n の中で交代群（偶置換の全体）A_n はいつでも正規部分群であることを証明せよ。

解答).A_n の任意の元は, 偶数個の互換の積でかける. $(i,j)^{-1} = (i,j)$ より, A_n は群. また S_n の任意の元 σ の遇奇に寄らず $\sigma A_n \sigma^{-1}$ の元は, 遇置換である. よって正規部分群である.

問題 1.5.8 群 G において、$Z(G) = \{a |\ ab = ba \text{ for any } b \in G\}$ とおく。$Z(G)$ を G の中心 (center) という。これに関して、次の事柄に証明を与えよ。

(a) $Z(G)$ はいつでも G の正規部分群である。

(b) $Z(G)$ に含まれる G の部分群 H は、G の正規部分群である。

(c) $H \subseteqq Z(G)$ が G の部分群であるとき、もし剰余群 G/H が巡回群ならば G はアーベル群である。

(d) 剰余群 $G/Z(G)$ がアーベル群ならば G 自身アーベル群である。

(証明)　(a) 任意の $x \in Z(G)$ と任意の $g \in G$ に対して, $gxg^{-1} = gg^{-1}x = x \in Z(G)$ を充たすので, $Z(G)$ は G の正規部分群である.
(b) 任意の $x \in H$ と任意の $g \in G$ に対して, $H \subset Z(G)$ により $gxg^{-1} = gg^{-1}x = x \in H$ を充たすので, H は G の正規部分群である.
(c) $G/H = \langle a^i H \rangle$ であるので, 任意の $x, y \in G$ に対して, ある $h, h' \in H$ を選ぶと, $x = a^i h, y = a^j h'$ と表わせる. $xy = (a^i h)(a^j h') = a^i (a^j h) h' = (a^j a^i)(h'h) = (a^j h')(a^i h) = yx$ により, G はアーベル群である.
(d) 任意の $x, y \in G$ に対して, ある $z, z' \in Z(G)$ を選ぶと, $(xy)(zz') = (xz)(yz') = (yz')(xz) = (yx)(z'z) = (yx)(zz')$ を充たす. 両辺に右から $(zz')^{-1}$ を掛けると $xy = yx$ が得られる. よって, G はアーベル群である.
[証明終]

問題 1.5.9 群 G の 2 元 a, b に対して、$[a,b] = aba^{-1}b^{-1}$ とおいてこれを a, b の交換子という。全ての G の交換子によって生成される G の部分群を $[G,G]$ と表し、G の交換子部分群という。これに関して、次の事柄に証明を与えよ。

(a) $[G,G]$ はいつでも G の正規部分群である。

(b) 剰余群 $G/[G,G]$ はアーベル群である。

(c) $H \subseteqq G$ が G の正規部分群であるとき、もし $[G,G] \subseteqq H$ ならば、剰余群 G/H はアーベル群である。

(d) 逆に剰余群 G/H がアーベル群となるような G の正規部分群 H については、$[G,G] \subseteqq H$ となる。

(証明) (a) 任意の $[a,b],[x,y] \in [G,G]$ に対して, $[a,b][x,y] \in [G,G]$ を充たす. $e = [e,e] \in [G,G]$ を選ぶと, 任意の $[a,b] \in [G,G]$ に対して, $[a,b][e,e] = [a,b]$ と $[e,e][a,b] = [a,b]$ を充たす. 任意の $[a,b] \in [G,G]$ に対して, $[b,a] \in [G,G]$ を選ぶと, $[a,b][b,a] = [e,e] = e$ と $[b,a][a,b] = [e,e] = e$ を充たす. よって, $[G,G]$ は G の部分群である. さらに, 任意の $[a,b] \in [G,G]$ と任意の $g \in G$ に対して, $g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gaba^{-1}g^{-1}b^{-1}bgb^{-1}g^{-1} = [ga,b][b,g] \in [G,G]$ により, $[G,G]$ は G の正規部分群である.
(b) $[a,b] = e$ ならば $ab = ba$ であることから, 明らかである.
(c) 自然な全射群準同型写像 $\pi : G/[G,G] \to G/H$ が存在し, さらに $G/[G,G]$ がアーベル群であることので, G/H もアーベル群である.
(d) 任意の $[x,y] \in [G,G]$ に対して, $xHyH = yHxH$ すなわち $xyH = yxH$ を充たすので, $[x,y] = xyx^{-1}y^{-1} \in H$ が成り立つ. [証明終]

問題 1.5.10 対称群 S_n について、その中心 $Z(S_n)$ と交換子群 $[S_n,S_n]$ を求めよ。

(解答) $Z(S_n) = \{\varepsilon\}$, 但し ε は恒等置換である. $[S_n,S_n] = A_n$.

1.6　準同型定理

「準同型定理の基本形」

- $f : G \to G'$ が群の全射準同型写像であるとき、$H = \mathrm{Ker}(f)$ と置くと、H は G の正規部分群で、f は自然な同型写像 $\overline{f} : G/H \to G'$ を導く。（任意の $[x] \in G/H$ に対して、$\overline{f}([x]) = f(x)$ と定義される。）

「準同型定理の色々な形」または「同型定理」

- $f : G \to G'$ が群の準同型写像であるとき、同型 $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$ がある。
- H と K が G の部分群で、K は正規部分群であるとする。$HK = \{h \cdot k |\ h \in H, k \in K\}$ は G の部分群であり、また $H \cap K$ は H の、K は HK の正規部分群である。このとき、$H/H \cap K \cong HK/K$ である。
- $K \subseteqq H \subseteqq G$ がそれぞれ G の部分群であるとき、H/K は G/K の正規部分群であり、$G/K \cong (G/K)/(H/K)$ である。

問題 1.6.1　「準同型定理の基本形」を証明せよ。

(証明)　(1) H が正規部分群であることを証明する.
任意の $a, b \in H$ に対して, $f(ab) = f(a)f(b) = e'$ により $ab \in H$ を充たす. よって H は G の部分群である. 任意の $x \in G$ と $y \in H$ に対して, $f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = f(x)e'f(x)^{-1} = e'$ により, H は G の正規部分群である.
(2) $\overline{f} : G/H \to G'$ が *well-defined* な写像であることを証明する.
$[x] = [y] \in G/H$ ならば, $x \in yH$ すなわち $y^{-1}x \in H$ を充たす. よって, $f(y)^{-1}f(x) = f(y^{-1}x) = e'$ により $f(x) = f(y)$ が成り立つ.
(3) $\overline{f} : G/H \to G'$ が単射であることを証明する.
$[x], [y] \in G/H$ に対して $f(x) = f(y)$ ならば, $y^{-1}x \in H$ により $[x] = [y]$ が成り立つ.
(4) $\overline{f} : G/H \to G'$ が全射であることを証明する.
f の全射性により導かれる.
(5) $\overline{f} : G/H \to G'$ が準同型写像であることを証明する.
任意の $[x], [y] \in G/H$ に対して, $\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y)\overline{f}([x])\overline{f}([y])$ が成り立つ.
以上により, $\overline{f} : G/H \to G'$ は同型写像である.　[証明終]

問題 1.6.2　「準同型定理の基本形」から「準同型定理の色々な形」を証明せよ。

(証明)　(1) $f : G \to G'$ が群の準同型写像であるとき, 同型 $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$ がある.
G' の部分群 $\mathrm{Im}(f)$ に対して, 「準同型定理の基本形」を適用すればよい.
(2) H と K が G の部分群で, K は正規部分群であるとする. $HK = \{h \cdot k |\ h \in H, k \in K\}$ は G の部分群であり, また $H \cap K$ は H の, K は HK の正規部分群である. このとき, $H/H \cap K \cong HK/K$ である.
$\varphi : H \to H/K; h \mapsto hK$ は準同型写像であり, $\mathrm{Ker}(\varphi) = H \cap K$ および $\mathrm{Im}(\varphi) = HK$ を充たしているので, (1) の結果を適用すればよい.

(3) $K \subseteqq H \subseteqq G$ がそれぞれ G の部分群であるとき，H/K は G/K の正規部分群であり，$G/H \cong (G/K)/(H/K)$ である．

$\psi : G/K \to G/H; gK \mapsto gH$ は全射準同型写像であり，$\mathrm{Ker}(\psi) = H/K$ を充たしているので，「準同型定理の基本形」を適用すればよい．　[証明終]

問題 1.6.3 n 次対称群 S_n の偶置換全体からなる部分群 A_n （交代群）は、正規部分群であり、$S_n/A_n \cong \mathbf{Z}/2\mathbf{Z}$ となる。このことを証明せよ。

(証明) 乗法群 $C_2 = \langle -1 \rangle \subset \mathbf{C}$ と加法群 $\mathbf{Z}/2\mathbf{Z}$ が同型であることは明らかである．よって以下では，$S_n/A_n \cong C_2$ が成り立つことを証明する．

$sgn : S_n \to C_2$ が群の全射準同型写像であることは明らかである．写像の定義により $\mathrm{Ker}(sgn) = A_n$ が成り立つ．準同型定理により A_n は S_n の正規部分群であり，$S_n/A_n \cong C_2$ が成り立つ．　[証明終]

問題 1.6.4 $SL(n, \mathbf{C})$ は $GL(n, \mathbf{C})$ の正規部分群であり、剰余群 $GL(n, \mathbf{C})/SL(n, \mathbf{C})$ は乗法群 $\mathbf{C}^\times = \mathbf{C} - \{0\}$ と同型であることを証明せよ。

(証明) $\det : GL(n, \mathbf{C}) \to \mathbf{C}^\times$ が群の全射準同型写像であることは明らかである．写像の定義により $\mathrm{Ker}(\det) = SL(n, \mathbf{C})$ が成り立つ．準同型定理により $SL(n, \mathbf{C})$ は $GL(n, \mathbf{C})S_n$ の正規部分群であり，$GL(n, \mathbf{C})/SL(n, \mathbf{C}) \cong \mathbf{C}^\times$ が成り立つ．　[証明終]

問題 1.6.5 $S = \{z \in \mathbf{C} |\ |z| = 1\}$ と置くと、S は乗法群 $\mathbf{C}^\times = \mathbf{C} - \{0\}$ の正規部分群である。このとき、$\mathbf{C}^\times/S$ はどのような群であるか？

(証明) $|\cdot| : \mathbf{C}^\times \to \mathbf{R}_+ := \{a \in \mathbf{R} |\ a > 0\ \}$ が群の全射準同型写像であることは明らかである．写像の定義により $\mathrm{Ker}(|\cdot|) = S$ が成り立つ．準同型定理により S は $\mathbf{C}^\times$ の正規部分群であり，$\mathbf{C}^\times/S \cong \mathbf{R}_+$ が成り立つ．　[証明終]

問題 1.6.6 n 次元実ベクトル空間 $\mathbf{R}^n$ は加法についてアーベル群と見なすことができる。このとき、$\mathbf{R}^n$ の原点を通る超平面 $H = \{(x_1, \ldots, x_n) \in \mathbf{R}^n |\ a_1x_1 + \cdots + a_nx_n = 0\}$ は $\mathbf{R}^n$ の正規部分群で、$\mathbf{R}^n/H \cong \mathbf{R}^1$ となることを示せ。ただし、ここで $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ である。

(証明) $a = (a_1, \ldots, a_n)$ と略記し，$\langle a, b \rangle$ で a と b の標準内積を表わす．このとき，$\langle a, \cdot \rangle : \mathbf{R}^n \to \mathbf{R}^1$ が群の全射準同型写像であることは明らかである．写像の定義により $\mathrm{Ker}(\langle a, \cdot \rangle) = H$ が成り立つ．準同型定理により H は $\mathbf{R}^n$ の正規部分群であり，$\mathbf{R}^n/H \cong \mathbf{R}^1$ が成り立つ．　[証明終]

問題 1.6.7 二つの整数 $n, m \in \mathbf{Z}$ について、$\mathbf{Z}$ の正規部分群 $n\mathbf{Z} = \{nz |\ z \in \mathbf{Z}\}$ と $m\mathbf{Z}$ を考える。

(a) $n\mathbf{Z} \subseteqq m\mathbf{Z}$ となるための必要十分条件は、n が m の倍数であることである。これを証明せよ。

(b) d を n と m の最大公約数、c を n と m の最小公倍数とおくと、$n\mathbf{Z} + m\mathbf{Z} = d\mathbf{Z}$, $n\mathbf{Z} \cap m\mathbf{Z} = c\mathbf{Z}$ となることを証明せよ。（とくに、n と m の任意の公約数は $an + bm$ $(a, b \in \mathbf{Z})$ という形に表されることに注意。）

(c) 同型定理から、$d\mathbf{Z}/m\mathbf{Z} \cong n\mathbf{Z}/c\mathbf{Z}$ となることを示せ。

(証明)　(a) $n\mathbf{Z} \subseteqq m\mathbf{Z}$ であると仮定するとき, $n = n\cdot 1 \in n\mathbf{Z} \subseteqq m\mathbf{Z}$ により, ある $\ell \in \mathbf{Z}$ を選ぶと, $n = m\ell$ を充たす. よって, n は m の倍数である. 逆に, n は m の倍数であると仮定すると, $n \in m\mathbf{Z}$ により, $n\mathbf{Z} \subseteqq m\mathbf{Z}$ が成り立つ.
(b) $n\mathbf{Z} + m\mathbf{Z} = d\mathbf{Z}$ はユークリッド互除法を用いることで確かめられる. $n\mathbf{Z} \cap m\mathbf{Z} = c\mathbf{Z}$ は意味を考えれば明らかである.
(c) (b) と同型定理により, $n\mathbf{Z}/c\mathbf{Z} = n\mathbf{Z}/(n\mathbf{Z}\cap m\mathbf{Z}) \cong (n\mathbf{Z}+m\mathbf{Z})/m\mathbf{Z} = d\mathbf{Z}/m\mathbf{Z}$ が成り立つ.　[証明終]

問題 1.6.8 S_4 の部分集合 $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ は、S_4 の正規部分群をなし、$S_4/V \cong S_3$ となることを示せ。

(証明)　任意の $\sigma \in S_4$ に対して, $\sigma(1)\sigma^{-1} = (1) \in S_4$, $\sigma(12)(34)\sigma^{-1} = (12)(34) \in S_4$, $\sigma(13)(24)\sigma^{-1} = (13)(24) \in S_4$, $\sigma(14)(23)\sigma^{-1} = (14)(23) \in S_4$ を充たすので, V は S_4 の正規部分群である.
準同型写像 $f : S_3 \to S_4/V$ を, 自然な埋め込み $S_3 \hookrightarrow S_4$ と自然な全射準同型写像 $S_4 \twoheadrightarrow S_4/V$ の合成写像として定義する. このとき, $\mathrm{Ker}(f) = V \cap S_3 = (1)$ により, f は単射である. また, $|S_4/V| = 6 = |S_3|$ により, f は全射である. よって, $S_4/V \cong S_3$ となる.　[証明終]

問題 1.6.9 G が有限群で、H と K がその部分群であるとき、もし指数 $[G : H]$ と $[G : K]$ が互いに素ならば、$G = HK$ となることを示せ。

(証明)　写像 $f : H \times K \to G; (h, k) \mapsto hk$ の像が HK である. $f(h_1, k_1) = f(h_2, k_2) \Leftrightarrow h_1k_1 = h_2k_2 \Leftrightarrow x := h_2^{-1}h_1 = k_2k_1^{-1} \in H\cap K \Leftrightarrow h_2 = h_1x^{-1}, k_2 = xk_1, x \in H\cap K$ が成り立つので, 任意の $hk \in HK$ に対して, $f^1(hk) = \{(hx^{-1}, xk)|\ x \in H\cap K\}$ を充たす. よって, 等式 $|H|\cdot|H| = |H\times K| = |HK|\cdot|H\cap K|$ が成り立つ. ここで, $[G : H]$ と $[G : K]$ は互いに素であり, $[G : H\cap K] = [G : H][H : H\cap K] = [G : K][K : H\cap K]$ が成り立つので, $[G : H]$ は $[K : H\cap K] \le [G : H]$ を割り切るので, $[G : H] = [K : H\cap K]$ が成り立つ. よって, 等式 $[G : H\cap K] = [G : K][G : H]$ が得られるので, $\frac{|G|}{|H\cap K|} = \frac{|G|}{|H|}\cdot\frac{|G|}{|K|}$ により, $|G| = \frac{|H|\cdot|K|}{|H\cap K|} = |HK|$ を充たす. 故に, $G = HK$ 成り立つ.　[証明終]

問題 1.6.10　(a) 与えられた二つの群 G_1 と G_2 に対して、集合 $G_1 \times G_2 = \{(g_1, g_2)|\ g_1 \in G_1, g_2 \in G_2\}$ に 2 項演算を $(g_1, g_2)\cdot(h_1, h_2) = (g_1\cdot h_1, g_2\cdot h_2)$ と定めることによって $G_1 \times G_2$ は群となる。これを G_1 と G_2 の直積という。$G_1 \times G_2$ の単位元は (e_1, e_2)、元 (g_1, g_2) の逆元は (g_1^{-1}, g_2^{-1}) である。以上のことを確かめよ。

(b) $G_1' = \{(g_1, e_2)|\ g_1 \in G_1\}$ は $G_1 \times G_2$ の正規部分群であり、$G_1 \times G_2/G_1' \cong G_2$ となることを証明せよ。同様に、 $G_1 \times G_2/G_2' \cong G_1$ である。

(c) $G = G_1\times G_2$ とおくとき、G の中心 $Z(G)$ と交換子部分群 $[G, G]$ について、$Z(G) = Z(G_1)\times Z(G_2)$, $[G, G] = [G_1, G_1] \times [G_2, G_2]$ が成り立つことを示せ。

(d) ある群 F があって、G_1 と G_2 がその正規部分群であるとき、直積 $G_1 \times G_2$ から F の部分群 G_1G_2 に自然な全射準同型 $\pi : G_1 \times G_2 \to G_1G_2$ が定義されることを示せ。また、$\mathrm{Ker}(\pi)$ はどのような部分群か？

(証明)　(a) 任意の $(g_1, g_2), (h_1, h_2), (f_1, f_2) \in G_1\times G_2$ に対して, $((g_1, g_2)\cdot(h_1, h_2))\cdot(f_1, f_2) = (g_1\cdot h_1, g_2\cdot h_2)\cdot(f_1, f_2) = ((g_1\cdot h_1)\cdot f_1, (g_2\cdot h_2)\cdot f_2) = (g_1\cdot(h_1\cdot f_1), g_2\cdot(h_2\cdot f_2)) = (g_1, g_2)\cdot(h_1\cdot f_1, h_2\cdot f_2) =$

$(g_1, g_2) \cdot ((h_1, h_2) \cdot (f_1, f_2))$ を充たす．$(e_1, e_2) \in G_1 \times G_2$ を選ぶと，任意の $(g_1, g_2) \in G_1 \times G_2$ に対して，$(g_1, g_2) \cdot (e_1, e_2) = (g_1, g_2) = (e_1, e_2) \cdot (g_1, g_2)$ を充たす．任意の $(g_1, g_2) \in G_1 \times G_2$ に対して，$(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$ を選ぶと，$(g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) = (e_1, e_2) = (g_1^{-1}, g_2^{-1}) \cdot (g_1, g_2)$ を充たす．以上により $G_1 \times G_2$ は群である．
(b) 自然な全射準同型写像 $f : G_1 \times G_2 \to G_2; (g_1, g_2) \mapsto g_2$ に対して，$\mathrm{Ker}(f) = G_1'$ であることは簡単に確かめられる．後は準同型定理を用いて，$(G_1 \times G_2)/G_1' \cong G_2$ が得られる．
(c) 定義により，明らかである．
(d) $\pi : G_1 \times G_2 \to G_1G_2; (g_1, g_2) \mapsto g_1g_2$ が全射であることは明らかである．$\pi((g_1, g_2))\pi((h_1, h_2)) = (g_1g_2)(h_1h_2) = (g_1g_2h_1g_2^{-1})(g_2h_2) \in G_1G_2$ を充たすので，準同型写像が定義できる．また，$\mathrm{Ker}(\pi) = G_1 \cap G_2$ である．　[証明終]

問題 1.6.11 H と K を G の部分群とする。このとき、次の 4 条件が同値であることを証明せよ。

(a) G の部分群 HK は（前問の (d) の写像 π によって）群として直積 $H \times K$ と同型である。

(b) HK の任意の元は $h \cdot k$ $(h \in H, k \in K)$ の形で一意的に表される。

(c) $a \cdot b = e$ $(a \in H, b \in K)$ ならば $a = b = e$ である。

(d) $H \cap K = \{e\}$

(証明)　(a) $\Rightarrow$ (b) 明らかである．
(b) $\Rightarrow$ (c) $a \cdot b = e = e \cdot e$ により，$a = b = e$ を充たす．
(c) $\Rightarrow$ (d) 任意の $a \in H \cap K$ に対して，$a \cdot a^{-1} = e$ であるから，$a = a^{-1} = e$ が成り立つ．
(d) $\Rightarrow$ (a) 問題 1.6.10 を適用することにより，明らかである．　[証明終]

問題 1.6.12 G が有限群で、H と K がその正規部分群であるとする。もし位数 $|H|$ と $|K|$ が互いに素ならば、$G \cong H \times K$ となることを証明せよ。
　とくに p と q が互いに素な整数であるとき、$\mathbf{Z}/(pq)\mathbf{Z} \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ である。

(証明)　部分群 $H \cap K$ の位数は，$|H|$ と $|K|$ の公約数であるから 1 である．すなわち $H \cap K = \{e\}$ である．問題 1.6.11 により，$HK = H \times K$ が得られる．また $|G| = |HK|$ により，$G \cong HK$ が得られるので，$G \cong H \times K$ が成り立つ．　[証明終]