

# 2014 年度 後期 代数学 1

担当 和地 輝仁

## 目次

1 シラバス抜粋	1
2 授業のノート	2
§1 整数の性質	2
§2 複素数	3
§3 群	5
§4 対称群	6
§5 演習問題	9
§6 問題の解答	11

## 1 シラバス抜粋

### 到達目標

1. 数の基本的な性質を知る。
2. 複素数の演算を実行できる。
3. 複素数の演算に、複素数平面を通して幾何的性質を利用できる。
4. 群の基本的な例を扱える。
5. 対称群の基本的な性質を、対称群の現れる実例に応用できる。

授業計画 順序を交換する場合もあるので注意すること。

- |               |             |
|---------------|-------------|
| 1. 整数の性質      | 9. 部分群      |
| 2. 実数の性質      | 10. 群の性質    |
| 3. 複素数        | 11. 対称群     |
| 4. 複素数の演算     | 12. 互換と巡回置換 |
| 5. 複素数の性質     | 13. 偶置換と奇置換 |
| 6. 複素数平面      | 14. 対称群の応用  |
| 7. 複素数平面と平面幾何 | 15. 期末試験    |
| 8. 群          |             |

成績評価 期末試験 (80%) と、毎回の演習問題の状況 (20%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

## 2 授業のノート

講義のノートの概略を記す。また、問題については、板書できなかったものも追加して記す。

### §1 整数の性質

(1.1) 整数 整数全体の集合  $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  は無限集合である。最大値、最小値はない。加法 (減法を含める) と乗法があり、加法の結合法則・交換法則、乗法の結合法則・交換法則、分配法則が成立する。

(1.2) 除法の定理 整数  $a$  と正整数  $b$  に対し、

$$a = bq + r \quad (0 \leq r < b)$$

を満たす整数  $q, r$  が一意的に存在する。

(1.3) 倍数・約数・公倍数・公約数・最小公倍数・最大公約数

(1) 0 以上の整数  $a, b$  が、 $a = bt$  ( $t$  は整数) を満たしているとき、 $a$  を  $b$  の倍数、 $b$  を  $a$  の約数と呼ぶ。

(2) 0 以上の整数  $m, n$  に対し、共通の倍数を公倍数、共通の約数を公約数と呼び、最小の公倍数を最小公倍数、最大の公約数を最大公約数と呼ぶ。

$m, n$  の最大公約数を  $(m, n)$  とも書く。 $(m, n) = 1$  のとき  $m$  と  $n$  は互いに素であると言う。 $(0, 0)$  は存在しない。

(1.4) 命題 0 以上の整数  $a, b$  の最小公倍数を  $l$  とし、また  $a = b = 0$  ではないときは最大公約数を  $g$  とする。

- (1)  $a, b$  の公倍数は  $l$  の倍数である。
- (2)  $a, b$  の公約数は  $g$  の約数である。

(1.5) 命題  $a, b$  を 0 以上の整数で、 $a$  と  $b$  の少なくとも一方は 0 ではないとし、 $a = b = 0$  でもないとする。

- (1) 非負整数  $g$  に対して、 $a = g\alpha, b = g\beta$  であるとき、 $g = (a, b)$  であることと、 $(\alpha, \beta) = 1$  であることは必要十分である。
- (2) 非負整数  $l$  に対して、 $l = a\alpha, l = b\beta$  であるとき、 $l$  が  $a$  と  $b$  の最小公倍数であることと、 $(\alpha, \beta) = 1$  であることは必要十分である。
- (3)  $g$  と  $l$  を、それぞれ、 $a$  と  $b$  の最大公約数と最小公倍数とすると、 $ab = gl$  である。

(1.6) 問題 512 と 768 の最大公約数と最小公倍数を求めよ。

(1.7) 補題  $a, b$  を互いに素な正整数、 $c$  を正整数とする。 $a$  が  $bc$  を割り切るならば  $a$  は  $c$  を割り切る。

(1.8) 素数・合成数 正の整数  $n$  が素数であるとは、 $n$  が 1 と  $n$  以外の約数を持たないことを言う。素数ではない正の整数を合成数と呼ぶ。ただし、1 は素数にも合成数にも含めない。

(1.9) 素因数分解の一意性 正の整数を素数の積に分解することを素因数分解と呼ぶ。素因数分解は、その順序を除いて一意的である。

(1.10) 命題

- (1)  $\sqrt{2}$  は無理数である。
- (2)  $\sqrt{3}$  は無理数である。
- (3) 正整数  $n$  が平方数ではないとき、 $\sqrt{n}$  は無理数である。

(1.11) エラトステネスのふるい 素数を得る効率的な方法。

(1.12) 定理 素数は無数にある。

(1.13) ユークリッドの互除法 正の整数  $a, b$  に対して、 $a$  を  $b$  で割った余りを  $r$  とすると、最大公約数に関する等式

$$(a, b) = (r, b)$$

が成立する。この等式を利用し、順に小さい数の最大公約数に変形して最大公約数を求めるアルゴリズムを、ユークリッドの互除法と呼ぶ。

(1.14) 例 ユークリッドの互除法を利用して 512 と 768 の最大公約数と最小公倍数を求めよ。

(1.15) ベズーの等式 整数  $a, b$  が互いに素ならば、

$$ax + by = 1$$

を満たす整数  $x, y$  が存在する。

(1.16) 問題 次の方程式を満たす整数解をすべて求めよ。

- (1)  $45x + 14y = 1$
- (2)  $45x - 14y = 1$
- (3)  $35x - 13y = 1$
- (4)  $35x - 13y = 2$
- (5)  $34x - 24y = 6$

## §2 複素数

(2.1) 定義 (複素数) 2乗して  $-1$  になる数を  $i$  で表し、虚数単位と呼ぶ。

$$i = \sqrt{-1}$$

$a > 0$  のとき  $\pm\sqrt{ai} = -a$  だから、 $\pm\sqrt{ai}$  は負数の平方根である。つまり、

$$\sqrt{-a} = \sqrt{ai} \quad (a > 0)$$

である。

実数  $a, b$  により、 $a + bi$  と書ける数を複素数と呼ぶ。 $a$  を実部、 $b$  を虚部と呼ぶ。実部が 0 である複素数を純虚数と呼ぶ。反対に虚部が 0 である複素数は実数である。

$a + bi = c + di$  ならば  $a = c$  かつ  $b = d$  である (複素数の相等)。

(2.2) 例 (和、差、積、複素数の相等) (1)–(3) は計算し簡単にせよ。(4)、(5) は実数  $x, y$  を決定せよ。

- (1)  $(2 + 3i) - (4 - 5i)$
- (2)  $(1 - 3i)(3 + 2i)$
- (3)  $i^3$
- (4)  $(x - y) + (2x + 3y)i = 3 + i$
- (5)  $(x + 2yi)(1 - 2i) = 7 - 9i$

(2.3) 共役複素数  $z = a + bi$  ( $a, b$  は実数) のとき、 $\bar{z} = a - bi$  を  $z$  の共役複素数と言う。 $z\bar{z}$  も  $z + \bar{z}$  も実数である。また、 $\bar{\bar{z}} = z$  ならば  $z$  は実数である。

(2.4) 複素数の除法  $\frac{z}{w}$  の分子・分母に  $\bar{w}$  を掛けて、 $\frac{z\bar{w}}{w\bar{w}}$  とすると分母が実数になるので、 $a + bi$  の形に書き直せる。

(2.5) 例 (除法) (1)  $\frac{1}{2 - 3i}$  (2)  $\frac{2 - 5i}{3 + 4i}$

(2.6) 注意 (大小関係、非零因子)

- (1) 複素数に大小関係はない。
- (2)  $zw = 0$  ならば  $z = 0$  または  $w = 0$  である。

(2.7) 複素数平面 複素数  $a + bi$  を  $xy$  平面の点  $(a, b)$  と同一視したものを複素数平面と呼ぶ。 $x$  軸を実軸、 $y$  軸を虚軸と呼ぶ。

共役複素数は、 $x$  軸対称の位置関係にある。複素数を  $-1$  倍すると、原点对称の位置に移動する。

(2.8) 絶対値  $z = a + bi$  のとき、 $|z| = \sqrt{a^2 + b^2}$  と定め、 $z$  の絶対値と呼ぶ。複素数平面における点  $z$  と原点との距離である。

$$|z|^2 = z\bar{z}, \quad |-z| = |z|, \quad |\bar{z}| = |z| \text{ を満たす。}$$

(2.9) 和と差の幾何的性質 複素数の和・差は、複素数平面でのベクトルの和・差に対応する。

(2.10) 実数倍の幾何的性質 複素数  $z$  と正の実数  $k$  に対して、 $kz$  は  $z$  を原点中心に  $k$  倍に拡大した点である。 $-kz$  は  $-z$  を原点中心に  $k$  倍に拡大した点である。

$$\text{実数 } k \text{ に対して、} |kz| = |k||z| \text{ を満たす。}$$

(2.11) 三角関数の復習 単位円周上の点  $P$  があり、半径  $OP$  が  $x$  軸からなす角を  $\theta$  とし、点  $P$  の座標を  $(x, y)$  とする。このとき、 $\cos \theta = x$ ,  $\sin \theta = y$  で定める。 $\theta$  が鋭角のときは、簡単な覚え方がある。

(2.12) 極形式  $z \neq 0$  のときのみ考える。半径  $Oz$  が実軸からなす角を  $\arg z$  と書き、 $z$  の偏角と呼ぶ。偏角は  $360^\circ \times n$  を足しても引いてもよいという自由度がある。

$z$  の極形式とは、 $z$  を次のように表示した形式のことである。

$$z = r(\cos \theta + i \sin \theta) \quad (\text{ただし } r = |z|, \theta = \arg z)$$

(2.13) 例 次の複素数を極形式で表せ。

$$(1) 1 + i \quad (2) -1 + i \quad (3) 1 + \sqrt{3}i \quad (4) 1 - \sqrt{3}i \quad (5) i \quad (6) -1$$

(2.14) 問題 ( $-z$  と  $1/z$  の極形式)  $z = r(\cos \theta + i \sin \theta)$  のとき、 $r$  と  $\theta$  を用いて、 $-z$  と  $\bar{z}$  と  $1/z$  を極形式で表せ。

(2.15) 加法定理

$$\sin(\alpha \pm \beta) = \sin \alpha \cos \beta \pm \cos \alpha \sin \beta,$$

$$\cos(\alpha \pm \beta) = \cos \alpha \cos \beta \mp \sin \alpha \sin \beta.$$

(2.16) 複素数の乗除

$$z_1 = r_1(\cos \theta_1 + i \sin \theta_1),$$

$$z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$$

のとき、

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)),$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)).$$

(2.17) 複素数の乗除と絶対値

$$|zw| = |z||w|, \quad \arg zw = \arg z + \arg w,$$

$$\left| \frac{z}{w} \right| = \frac{|z|}{|w|}, \quad \arg \frac{z}{w} = \arg z - \arg w,$$

(2.18) 乗除の幾何的性質 ある複素数  $w$  に、 $z = r(\cos \theta + i \sin \theta)$  を掛けると、 $zw$  は  $w$  を原点中心に  $\theta$  回転し、 $r$  倍に拡大した点である。

特に、 $iw$  は  $w$  を原点中心に  $90^\circ$  回転した点であり、 $-iw$  は  $w$  を原点中心に  $-90^\circ$  回転した点である。

(2.19) 例 (乗除と幾何)

(1)  $2 + i$  を原点の回りに  $60^\circ$  回転した点を求めよ。

(2) 原点と  $2 + i$  を頂点に持つ正方形の、残り 2 つの頂点を求めよ。

(2.20) ド・モアブルの定理

$$\begin{aligned}(\cos \theta + i \sin \theta)^n &= \cos n\theta + i \sin n\theta, \\(r(\cos \theta + i \sin \theta))^n &= r^n(\cos n\theta + i \sin n\theta),\end{aligned}$$

(2.21) 例 計算して簡単にせよ。

- (1)  $(1 + i)^{10}$
- (2)  $(\sqrt{3} + i)^{12}$

(2.22)  $n$  乗根 複素数の範囲で、1 の  $n$  乗根は、

$$\cos \frac{k}{n} \times 360^\circ + i \sin \frac{k}{n} \times 360^\circ \quad (k = 0, 1, \dots, n-1)$$

の  $n$  個である。

例えば、1 の 5 乗根は、単位円周上、1 から始めて  $72^\circ$  ごとに円周を 5 等分した点たちである。

(2.23) 例 ( $n$  乗根)

- (1) 1 の 3 乗根は、 $\cos \theta + i \sin \theta$  ( $\theta = 0^\circ, 120^\circ, 240^\circ$ ) だから、 $1, \frac{-1 + \sqrt{3}i}{2}, \frac{-1 - \sqrt{3}i}{2}$  の 3 つである。
- (2) 2 の 4 乗根は、 $\sqrt[4]{2}(\cos \theta + i \sin \theta)$  ( $\theta = 0^\circ, 90^\circ, 180^\circ, 270^\circ$ ) だから、 $\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i$  の 4 つである。

(2.24) 例  $n$  を 2 以上の整数とし、 $\theta = 360^\circ/n$ ,  $z = \cos \theta + i \sin \theta$  とおく。このとき、次を証明せよ。

- (1)  $1 + z + z^2 + \dots + z^{n-1} = 0$
- (2)  $1 + \cos \theta + \cos 2\theta + \dots + \cos(n-1)\theta = 0$
- (3)  $\sin \theta + \sin 2\theta + \dots + \sin(n-1)\theta = 0$

(2.25) 例 (ナポレオンの定理) 三角形 ABC の外側に、各辺を 1 辺にもつ正三角形を合計 3 つ作る。3 つの正三角形の重心は正三角形の頂点をなす。

### §3 群

(3.1) 定義 (群) 集合  $G$  が群であるとは、 $G$  に演算  $a \cdot b$  ( $a, b \in G$ ) が定義されており、次の条件を満たすことをいう。

- (G1)  $(ab)c = a(bc)$  ( $a, b, c \in G$ ) (結合法則)
- (G2) ある元  $e \in G$  が存在して、任意の  $a \in G$  に対して  $ea = ae = a$  を満たす。このような元  $e$  を単位元という。
- (G3) 任意の  $a \in G$  に対して、 $b \in G$  が存在して  $ab = ba = e$  を満たす。このような  $b$  を  $a$  の逆元といい、 $a^{-1}$  と書く。

(3.2) 注意 (単位元、逆元の一意性)

- (1) 単位元は一意的である。
- (2) 逆元は一意的である。
- (3) 結合法則があるので、3 つ以上の元の積も単に  $abc$  と書いてよい。

例えば、整数の集合  $\mathbb{Z}$  に、 $a * b = a + 2b$  と演算を定義すると結合法則を満たさないので、 $(a * b) * c$  とか  $a * (b * c)$  と書かなくてはならない。

(3.3) 定義 (アーベル群、位数) 群  $G$  が、(G4)  $ab = ba$  ( $a, b \in G$ ) (交換法則)を満たすとき、 $G$  をアーベル群と呼ぶ。

また、群  $G$  の元の個数を位数とよぶ。位数が有限の群を有限群、無限の群を無限群とよぶ。

(3.4) 例 (数のなす群) ここでは、簡単のために、集合  $G$  に演算  $*$  を考えることを  $(G, *)$  と表す。

- (1)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  は群である。
- (2)  $(\mathbb{Q}^+, +)$ ,  $(\mathbb{R}, \times)$  は群ではない。
- (3)  $(\mathbb{Q}^\times, \times)$ ,  $(\mathbb{R}^\times, \times)$ ,  $(\mathbb{C}^\times, \times)$  は群である。
- (4)  $(\{1, -1\}, \times)$ ,  $(\{\pm 1, \pm i\}, \times)$  は群である
- (5)  $(\mathbb{T}, \times)$  は群である。

(3.5) 例 (変換のなす群) 次のような平面図形または空間図形について、その図形を自分自身に写すような合同変換全体は群をなす。角かっこ内はその群の位数である。ただし、平面図形の裏返しや空間図形の鏡映を含めない場合の位数である。それらを含めると位数は倍になる。

- (1) 正三角形ではないような二等辺三角形 [1]
- (2) 正三角形 [3]
- (3) 正方形ではないような長方形 [2]
- (4) 正方形 [4]
- (5) 正  $n$  角形 [ $n$ ]
- (6) 正四面体 [12]
- (7) 立方体 [24]
- (8) 正八面体 [24]
- (9) 正十二面体 [60]
- (10) 正二十面体 [60]

(3.6) 定義 (部分群) 群  $G$  の部分集合  $H$  が、 $G$  と同じ演算に関して群であるとき、 $H$  を  $G$  の部分群という。

(3.7) 例 (部分群)

- (1)  $\{e\}$ ,  $G$  はともに  $G$  の部分群である。これらは自明な部分群と呼ばれる。
- (2)  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$  は和に関して部分群の列である。

(3)  $\mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$  は積に関して部分群の列である。

(4)  $\mathbb{Q}^\times \subset \mathbb{Q}$  はともに群であるが、異なる演算に関する群なので、部分群の関係にはない。

(5)  $\mathbb{T} \subset \mathbb{C}^\times$  は部分群である。

(3.8) 問題  $H = \{1, -1, i, -i\}$  は、 $\mathbb{C}^\times$  の部分群であることを示せ。ただし、 $i$  は虚数単位を表す。

(3.9) 問題 (部分群の共通部分は再び部分群) 群  $G$  の 2 つの部分群  $H_1$  と  $H_2$  があるとき、 $H_1 \cap H_2$  も  $G$  の部分群であることを示せ。

(3.10) 定理 (部分群であるための必要十分条件) 群  $G$  とその空ではない部分集合  $H$  があるとき、次の条件は同値である。

- (i)  $H$  は  $G$  の部分群である。
- (ii) 任意の  $a, b \in H$  に対して、 $ab \in H$  かつ  $a^{-1} \in H$ 。
- (iii) 任意の  $a, b \in H$  に対して、 $a^{-1}b \in H$ 。

## §4 対称群

(4.1) 定義 (対称群) 正整数  $n$  に対して、1 から  $n$  までの整数の集合を  $\Omega$  と置く。全単射  $\sigma : \Omega \rightarrow \Omega$  を  $n$  文字の置換と呼ぶ。置換  $\sigma$  が、1 を  $i_1$  に、2 を  $i_2$  に、 $\dots$ ,  $n$  を  $i_n$  に写すとき、

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \quad (1)$$

と書く。

$n$  文字の置換全体の集合を  $S_n$  と書き、 $S_n$  上の演算を次で定める。 $\sigma, \tau \in S_n$  のとき、 $n$  文字の置換  $\sigma\tau$  を

$$(\sigma\tau)(i) = \sigma(\tau(i)) \quad (i = 1, 2, \dots, n)$$

で定める (順番注意! つまり、 $\tau$  で写してから、さらに、 $\sigma$  で写す置換)。この演算に関して  $S_n$  は群をなし、 $S_n$  は  $n$  次対称群と呼ばれる。

(4.2) 問題 ( $S_n$  の位数)

- (1)  $n$  次対称群  $S_n$  の位数 (元の個数) は  $n!$  であることを示せ。
- (2)  $S_n$  の単位元を答えよ。  $S_n$  の単位元は恒等置換と呼ばれ、 $e$  と書く。
- (3)  $\sigma, \tau \in S_n$  に対して、 $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$  であることを示せ。

(4.3) 問題 (積と逆元) 4 次対称群  $S_4$  について答えよ。

- (1)  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$  の逆元を求めよ。
- (2)  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$  の積  $\sigma\tau$  を求めよ。

(4.4) 定義 (巡回置換, 互換) 1 から  $n$  までの整数のうち、異なる  $k$  個  $i_1, i_2, \dots, i_k$  が与えられたとする (大小関係は任意でよい)。このとき、 $i_1$  を  $i_2$  に写し、 $i_2$  を  $i_3$  に写し、 $\dots$ ,  $i_{k-1}$  を  $i_k$  に写し、 $i_k$  は  $i_1$  に写して、他の数は動かさないような置換を長さ  $k$  の巡回置換と呼び、 $(i_1 i_2 \cdots i_k)$  と書く。特に、長さ 2 の巡回置換  $(a b)$  を互換と呼び、 $(a a+1)$  の形の互換を隣接互換と呼ぶ。

長さ  $k$  の巡回置換の表示は、どの数から書き始めるかにより  $k$  通りある。例えば、 $(a b)$  と  $(b a)$  は同じ互換を表す。

(4.5) 問題 (互換、巡回置換の積)  $S_6$  について答えよ。

- (1) 互換の積  $(1 2)(2 3)$  を計算し、式 (1) のように表示せよ。
- (2) 互換の積  $(1 2)(2 3)(1 2)$  を計算し、互換の形で表せ。
- (3) 巡回置換の積  $(1 2 3)(2 4 6)$  を計算し、式 (1) のように表示せよ。

(4.6) 定義 (置換のベキ)  $\sigma \in S_n$  に対して、 $\sigma$  を  $k$  個掛け合わせたものを、 $\sigma^k$  と書く。また、 $\sigma$  の逆元  $\sigma^{-1}$  を  $k$  個掛け合わせたものを、 $\sigma^{-k}$  と書く。

(4.7) 問題 (置換のベキ)  $S_n$  について答えよ。

- (1) 互換  $\sigma = (a b)$  に対して、 $\sigma^2$  と  $\sigma^{-1}$  を求めよ。
- (2) 長さ  $k$  の巡回置換  $\sigma$  に対して、 $\sigma^k$  を求めよ。
- (3) 長さ  $k$  の巡回置換  $\sigma = (i_1 i_2 \cdots i_k)$  の逆元を巡回置換で表せ。
- (4) # 長さ  $k$  の巡回置換  $\sigma$  に対して、 $\sigma^2$  が再び巡回置換になるための条件を求めよ。

## (4.8) 定理 (置換の隣接互換の積への分解)

- (1) 互換は隣接互換の積で表せる。
- (2) 巡回置換は互換の積で表せる。
- (3) 置換は巡回置換の積で表せる。従って、隣接互換の積で表せる。

*Proof.* (1)  $a < b$  のとき互換  $(a b)$  を考えると、

$$(a b) = (a a+1)(a+1 a+2) \cdots (b-2 b-1) \cdot (b-1 b) \\ \cdot (b-2 b-1)(b-3 b-2) \cdots (a a+1)$$

であるから、互換は隣接互換の (奇数個の) 積で書ける。

(2) 巡回置換  $(i_1 i_2 \cdots i_k)$  を考えると、

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k)$$

であるから、巡回置換は互換の積で書ける。

(3) 置換  $\sigma \in S_n$  をとる。まず、 $\{1, 2, \dots, n\}$  のうち 1 つの数をとり  $i_1$  とする。 $i_2 = \sigma(i_1), i_3 = \sigma(i_2), \dots$  と  $i_a$  を取っていくと、いずれ  $i_1$  に戻るので、それらの数で巡回置換  $\tau_1 = (i_1 i_2 \cdots i_k)$  を構成する。次に、まだ使われていない数  $j_1$  をとり、同様に巡回置換  $\tau_2 = (j_1 j_2 \cdots j_l)$  を構成する。ここで、 $\tau_1$  と  $\tau_2$  には共通する数がないので可換であることに注意しておく。このように、数を使い切るまで巡回置換を構成すると、 $\sigma = \tau_1 \tau_2 \cdots \tau_m$  の形に書けるから、置換は巡回置換の積で書ける。  $\square$

つまり、どんな置換を与えるあみだくじも、隣合う縦線の間に横棒を何本か引けば作ることができる。

(4.9) 問題 (互換の積への分解) 次の問に答えよ。

(1) 巡回置換  $(1\ 4\ 2\ 3)$  を互換の積で表せ。また、隣接互換の積で表せ。

(2) 置換  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$  を互換の積で表せ。また、隣接互換の積で表せ。

(4.10) 定義 (転倒数) 順列  $i_1, i_2, \dots, i_n$  の転倒数とは、 $i_a > i_b$  ( $a < b$ ) となっている組の総数のことである。

また、置換

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

の転倒数を、順列  $i_1, i_2, \dots, i_n$  の転倒数で定める。

例えば、置換  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$  においては、1 より左に 3, 5, 4 があり、2 より左に 3, 5, 4 があり、4 より左に 5 があるから転倒数は、7 である。

(4.11) 問題 次の問に答えよ。

(1) 隣接互換の転倒数を求めよ。

(2)  $\sigma \in S_n$  の転倒数と、その逆元  $\sigma^{-1}$  の転倒数は等しいことを示せ。

(4.12) 定理 (隣接互換の積での表示の個数の偶奇)

(1)  $\sigma \in S_n$  とし、 $\tau = (a\ a+1)$  を隣接互換とする。このとき、 $\sigma\tau$  の転倒数は、 $\sigma$  の転倒数より 1 多いか 1 少ないかのいずれかである。

(2)  $\sigma \in S_n$  を隣接互換の積で表したとき、その個数の偶奇は表し方によらず、 $\sigma$  の転倒数の偶奇に一致する (個数は表し方によるので注意)。

Proof. (1)  $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$  とすると、

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} (a\ a+1) = \begin{pmatrix} 1 & \cdots & a & a+1 & \cdots & n \\ i_1 & \cdots & i_{a+1} & i_a & \cdots & i_n \end{pmatrix}$$

である。 $\sigma$  と  $\sigma\tau$  において、転倒の有無が変化する組は、 $i_a, i_{a+1}$  の組のみである。よって、 $i_a < i_{a+1}$  ( $i_a > i_{a+1}$ ) のときは、 $\sigma\tau$  の転倒数が  $\sigma$  の転倒数より 1 大きい (小さい)。

(2) 隣接互換の奇数個 (偶数個) の積ならば、転倒数は奇数 (偶数) であることが (1) よりわかる。しかし転倒数、したがって転倒数の偶奇は隣接互換の積による表し方によらず決まるので、積の個数の偶奇も隣接互換の積による表し方によらず決まる。□

(4.13) 定義 (奇置換・偶置換) 偶数個の隣接互換の積で表せる置換を偶置換。奇数個の隣接互換の積で表せる置換を奇置換という。

次の問題によれば、偶置換 (奇置換) を、偶数個 (奇数個) の互換の積で表せる置換、と定義しても同じことである。

(4.14) 問題

(1) 互換は奇置換であることを示せ。

(2) 偶置換と偶置換の積、および、奇置換と奇置換の積は偶置換であることを示せ。また偶置換と奇置換の積は奇置換であることを示せ。

(4.15) 定理  $\sigma \in S_n$  を隣接互換の積で表す最小個数は、 $\sigma$  の転倒数に一致する。

Proof. まず、 $\sigma \in S_n$  を隣接互換の積で表したとき、その個数は最低でも  $\sigma$  の転倒数だけ必要であることは、(4.8) よりわかる。

また、転倒数の個数での表し方があることも以下のようにわかる。 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$  において、 $i_a > i_{a+1}$  となる箇所があれば、隣接互換を右から掛けて  $\sigma(a\ a+1)$  を考えると、 $\sigma$  よりも転倒数が 1 小さくなる。このように転倒数を 1 ずつ減少させていくと、いずれ単位元に到達し、

$$\sigma\tau_1\tau_2\cdots\tau_k = e \quad (\tau_j \text{ は隣接互換})$$

となり、このとき  $k$  は  $\sigma$  の転倒数である。従って、 $\sigma = \tau_k \cdots \tau_2\tau_1$  と  $\sigma$  を転倒数の個数の隣接互換の積で表せた。□



(4.16) 例 (あみだくじ) 縦線が  $n$  本あるあみだくじは、 $n$  文字の置換と対応する。(4.8)により、どんな入れ替えをするあみだくじも、隣り合う縦線の間にかかれる横棒だけで実現できる。(4.12)により、同じ結果を与えるあみだくじどうしでは、横棒の本数の偶奇は一致する。(4.15)により、ある置換に対応するあみだくじの(隣接縦線間の)横棒の最小本数は、その置換の転倒数に等しい。

(4.17) 例 (15 パズル) いわゆる 15 パズルは、下図左の初期状態からどう動かしても下図右のようにはできない。

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

パズルの 1 行目を左から右へたどって数字を拾い、次に 2 行目は右から、3 行目は左から、4 行目は右から順に数字を拾ってできる数列を考える。例えば、上図左ならば、1, 2, 3, 4, 8, 7, 6, 5, 9, 10, 11, 12, 15, 14, 13 を考える。パズルのピースを 1 度ずらしてこの数列が変化しても(しなくても)、この数列の転倒数の偶奇が変わらないので、転倒数が偶数の上図左から奇数の上図右にはできないことがわかる。

(4.18) 問題 # (交代群)  $S_n$  の偶置換だけを集めた部分集合を  $A_n$  と書き、 $n$  交代群と呼ぶ。このとき、次の問に答えよ。

- (1)  $A_n$  の位数は  $n!/2$  であることを示せ。
- (2)  $A_n$  は  $S_n$  の部分群であることを示せ。

(4.19) 定義 # ( $\text{sgn } \sigma$ ) 置換  $\sigma$  に対して、

$$\text{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ は偶置換} \\ -1 & \sigma \text{ は奇置換} \end{cases}$$

で定める  $\text{sgn}(\sigma)$  を、置換  $\sigma$  の符号と言う。

## §5 演習問題

(5.1) 問題 素数の定義を言え。

(5.2) 問題  $\sqrt{2}$  が無理数であることを、素因数分解の一意性を用いて証明せよ。

(5.3) 問題 ユークリッドの互除法を用いて、次の 2 数の最大公約数と最小公倍数を求めよ。

- (1) 336, 360
- (2) 448, 588

(5.4) 問題 次の方程式を満たす整数解  $x, y$  を 1 組求めよ。

- (1)  $39x + 28y = 1$
- (2)  $28x - 11y = 1$
- (3)  $39x - 11y = -3$

(5.5) 問題 次の複素数を計算し簡単にせよ。

- (1)  $(1+i) - (2-i)$
- (2)  $(1+i)(2-i)$
- (3)  $\frac{1+i}{2-i}$

(5.6) 問題 次の文章のおかしな箇所を指摘せよ。

「 $x$  の 2 次方程式  $x^2 + x + 1 = 0$  の 2 つの解を  $\alpha, \beta$  ( $\alpha \leq \beta$ ) と置くと、解と係数の関係より、 $\alpha\beta = 1$  である。」

(5.7) 問題 複素数  $z = 2 - i$  に対して次を求めよ。

- (1)  $|z|$
- (2)  $\bar{z}$
- (3)  $z$  の実部
- (4)  $z$  の虚部

(5.8) 問題 次の複素数を極形式で書け。

- (1)  $1+i$
- (2)  $1-\sqrt{3}i$
- (3)  $-\sqrt{3}-3i$
- (4)  $-\sqrt{2}+\sqrt{2}i$

(5.9) 問題 次の問に答えよ。

- (1) 複素数  $2 - i$  を原点中心に  $30^\circ$  回転した点を求めよ。
- (2) 複素数  $2 - i$  を原点中心に  $315^\circ$  回転した点を求めよ。

(5.10) 問題 次の複素数を計算し、 $a + bi$  の形で書け。

- (1)  $(1 + \sqrt{3}i)^6$     (2)  $(1 - i)^9$

(5.11) 問題 次の問に答えよ。

- (1) すべての 1 の 8 乗根を、 $a + bi$  の形で書き、複素数平面上に図示せよ。
- (2) すべての 1 の 5 乗根を、極形式で書け。

(5.12) 問題 次の問に答えよ。

- (1) 集合  $G$  が群であることの定義を書け。
- (2) 次の集合は、指定された演算に関して群か否か。
  - (a)  $(\mathbb{Z}, +)$     (b)  $(\mathbb{Q}, +)$     (c)  $(\mathbb{R}, +)$     (d)  $(\mathbb{C}, +)$     (e)  $(\mathbb{Q}^\times, \times)$
  - (f)  $(\mathbb{R}^\times, \times)$     (g)  $(\mathbb{C}^\times, \times)$

(5.13) 問題 次の図形における合同変換はいくつあるか言え。ただし、合同変換には裏返しをするものも含めることとする。

- (1) 正 5 角形
- (2) 半円
- (3) 底面が正三角形である三角柱
- (4) 正 12 面体

(5.14) 問題 正 4 面体の 4 頂点に、1, 2, 3, 4 と名前を付ける。この正 4 面体の合同変換を、変換前の頂点番号を上段に、変換後を下段に書いて、

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

のように表すことにする。これは、頂点 4 を通る軸の回りの回転である。

- (1) 合同変換のうち、頂点 2 を通る軸の回りの回転は、 $0^\circ$ ,  $120^\circ$ ,  $240^\circ$  回転の 3 つあるが、このうち恒等変換ではないものを上の形で書け。
- (2) 合同変換  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$  の逆元を書け。
- (3) 合同変換の積  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$  を計算せよ。

(5.15) 問題 次の問に答えよ。

- (1) 対称群とは何か。
- (2) 5 次対称群はいくつの元を含むか。
- (3) 5 次対称群の元  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$  の逆元を言え。
- (4) 4 次対称群の元の積  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$  を求めよ。
- (5) 3 次対称群の恒等置換を書け。

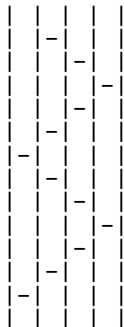
(5.16) 問題 次の問に答えよ。

- (1) 5 次対称群に属する置換  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$  を互換の積で表せ。
- (2) 上の置換を隣接互換の積で表せ。
- (3) 上の置換の転倒数を求めよ。
- (4) 上の置換を最も少ない個数の隣接互換の積で表せ。

(5.17) 問題 次の問に答えよ。

- (1) 置換を互換の積で書いたときの、互換の個数の性質を、「偶奇」の語を用いて 15 字以内で書け。
- (2) 前の問題の置換は偶置換か、奇置換か。

(5.18) 問題 図のあみだくじと同じ結果をもたらすあみだくじは、最小でも横棒が何本必要か。また、その最小本数で実現されたあみだくじを書け。



### §6 問題の解答

(1.6) の解答

$$768 \div 512 = 1 \text{ あまり } 256,$$

$$512 \div 256 = 1 \text{ あまり } 0$$

だから、 $(768, 512) = (256, 512) = (256, 0) = 256$ .

(1.16) の解答 (1)  $(x, y) = (5, -16)$  (2)  $(x, y) = (5, 16)$  (3)  $(x, y) = (3, 8)$

(4)  $(x, y) = (6, 16)$  (5)  $(x, y) = (15, 21)$

(5.1) の解答 1 と自分自身の他に約数のないような正整数。ただし、1 は素数には含めない。

(5.2) の解答  $\sqrt{2} = a/b$  ( $a, b$  は正整数) と表せたと仮定して背理法で証明する。 $a = p_1 p_2 \cdots p_k, b = q_1 q_2 \cdots q_l$  をそれぞれ素因数分解とする ( $p_i, q_j$  は素数) と、 $2b^2 = a$  より、

$$2q_1^2 q_2^2 \cdots q_l^2 = p_1^2 p_2^2 \cdots p_k^2$$

となる。左辺は奇数個、右辺は偶数個の素数の積だから、素因数分解の一意性に矛盾する。よって  $\sqrt{2}$  は無理数である。

(5.3) の解答 (1) 最大公約数は 24. 最小公倍数は、 $336 \times 360 \div 24 = 5040$ .

(2) 最大公約数は 28. 最小公倍数は 9408.

(5.4) の解答 (1)

$$39 \div 28 = 1 \text{ あまり } 11 \qquad \text{より } 11 = 39 - 28, \qquad (a)$$

$$28 \div 11 = 2 \text{ あまり } 6 \qquad \text{より } 6 = 28 - 11 \cdot 2, \qquad (b)$$

$$11 \div 6 = 1 \text{ あまり } 5 \qquad \text{より } 5 = 11 - 6, \qquad (c)$$

$$6 \div 5 = 1 \text{ あまり } 1 \qquad \text{より } 1 = 6 - 5. \qquad (d)$$

したがって、

$$1 \stackrel{d}{=} 6 - 5$$

$$\stackrel{c}{=} 6 - (11 - 6) = 6 \cdot 2 - 11$$

$$\stackrel{b}{=} (28 - 11 \cdot 2) \cdot 2 - 11 = 28 \cdot 2 - 11 \cdot 5$$

$$\stackrel{a}{=} 28 \cdot 2 - (39 - 28) \cdot 5 = 28 \cdot 7 - 39 \cdot 5.$$

よって、 $(x, y) = (-5, 7)$ .

(2)

$$28 \div 11 = 2 \text{ あまり } 6 \qquad \text{より } 6 = 28 - 11 \cdot 2, \qquad (a)$$

$$11 \div 6 = 1 \text{ あまり } 5 \qquad \text{より } 5 = 11 - 6, \qquad (b)$$

$$6 \div 5 = 1 \text{ あまり } 1 \qquad \text{より } 1 = 6 - 5. \qquad (c)$$

したがって、

$$1 \stackrel{c}{=} 6 - 5$$

$$\stackrel{b}{=} 6 - (11 - 6) = 6 \cdot 2 - 11$$

$$\stackrel{a}{=} (28 - 11 \cdot 2) \cdot 2 - 11 = 28 \cdot 2 - 11 \cdot 5.$$

よって、 $(x, y) = (2, 5)$ .

(3)

$$39 \div 11 = 3 \text{ あまり } 6 \qquad \text{より } 6 = 39 - 11 \cdot 3, \qquad (a)$$

$$11 \div 6 = 1 \text{ あまり } 5 \qquad \text{より } 5 = 11 - 6, \qquad (b)$$

$$6 \div 5 = 1 \text{ あまり } 1 \qquad \text{より } 1 = 6 - 5. \qquad (c)$$

したがって、

$$1 \stackrel{c}{=} 6 - 5$$

$$\stackrel{b}{=} 6 - (11 - 6) = 6 \cdot 2 - 11$$

$$\stackrel{a}{=} (39 - 11 \cdot 3) \cdot 2 - 11 = 39 \cdot 2 - 11 \cdot 7.$$

よって、両辺  $-3$  倍すると、 $(x, y) = (-6, -21)$  がわかる。

(5.5) の解答 (1)  $-1 + 2i$  (2)  $3 + i$  (3)  $\frac{1 + 3i}{5}$

(5.6) の解答 複素数には大小関係がないので、 $\alpha \leq \beta$  がおかしい。

(5.7) の解答 (1)  $5$  (2)  $2 + i$  (3)  $2$  (4)  $-1$

(5.8) の解答 (1)  $\sqrt{2}(\cos 45^\circ + i \sin 45^\circ)$  (2)  $2(\cos 300^\circ + i \sin 300^\circ)$  (3)  $2\sqrt{3}(\cos 210^\circ + i \sin 210^\circ)$  (4)  $2(\cos 135^\circ + i \sin 135^\circ)$

(5.9) の解答 (1)  $(2 - i)(\cos 30^\circ + i \sin 30^\circ) = (2 - i)\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = \frac{2\sqrt{3} + 1}{2} - \frac{2 + \sqrt{3}}{2}i.$

(2)  $(2 - i)(\cos 315^\circ + i \sin 315^\circ) = (2 - i)\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right) = \frac{1 - 3i}{\sqrt{2}}$  (あるいは  $\frac{\sqrt{2}}{2} - \frac{3\sqrt{2}}{2}i$ ).

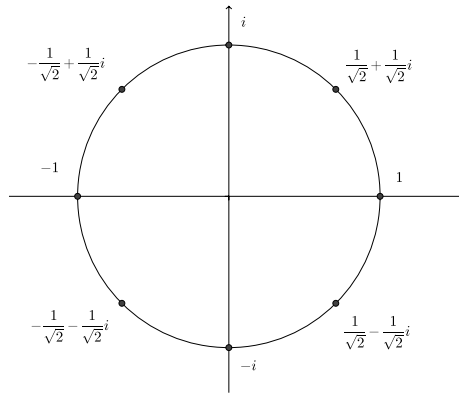
(5.10) の解答 (1)

$$(1 + \sqrt{3})^6 = (2(\cos 60^\circ + i \sin 60^\circ))^6 = 2^6(\cos 360^\circ + i \sin 360^\circ) = 2^6 = 64.$$

(2)

$$\begin{aligned} (1 - i)^9 &= \left(\sqrt{2}(\cos(-45^\circ) + i \sin(-45^\circ))\right)^9 \\ &= (\sqrt{2})^9(\cos(-405^\circ) + i \sin(-405^\circ)) \\ &= (\sqrt{2})^9(\cos(-45^\circ) + i \sin(-45^\circ)) \\ &= (\sqrt{2})^9\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i\right) \\ &= (\sqrt{2})^8(1 - i) = 16(1 - i). \end{aligned}$$

(5.11) の解答 (1) 1 の 8 乗根は  $\cos \theta + i \sin \theta$  ( $\theta = \frac{360^\circ}{8} \times k, k = 0, 1, \dots, 7$ ) だから、 $\theta = 45^\circ \times k$  ( $k = 0, 1, \dots, 7$ ) である。よって、すべての 1 の 8 乗根は、 $1, \frac{1+i}{\sqrt{2}}, i, \frac{-1+i}{\sqrt{2}}, -1, \frac{-1-i}{\sqrt{2}}, -i, \frac{1-i}{\sqrt{2}}$  である。図は下のとおり。



(2)  $\cos \theta + i \sin \theta$  ( $\theta = 0^\circ, 72^\circ, 144^\circ, 216^\circ, 288^\circ$ ).

(5.12) の解答 (1) (3.1) を見よ。(2) すべて群である。

(5.13) の解答

- (1) 1つの頂点の写る先が5通り、その隣の頂点の写る先が2通りだから、10通り。
- (2) 直径の端点の写る先が2通りだから、2通り。
- (3) 底面の1つの頂点の写る先が6通り、その底面で隣の頂点の写る先が2通りだから、12通り。
- (4) 正12面体には20頂点あり、各頂点からは稜が3本ずつ出ていることに注意しておく。1つの頂点の写る先が20通り、その隣の頂点の写る先が3通りだから、60通り。

(5.14) の解答 (1)  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

(2) 2行で表示した合同変換の、下の行の番号の頂点を、その上にある番号の頂点に写せばよいから、 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ .

(3)  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

(5.15) の解答 (1) (4.1) を見よ。(2)  $5! = 120$ .

(3)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

(4)  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

(5)  $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

(5.16) の解答 (1)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 4)(2\ 5) = (1\ 3)(3\ 4)(2\ 5)$ .

(2) (1) から続けて、 $(1\ 3)(3\ 4)(2\ 5) = (1\ 2)(2\ 3)(1\ 2) \cdot (3\ 4) \cdot (2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)$ .

(3) 7 (このあたり授業ではやっていないかも知れません)

(4)  $(2\ 3)(1\ 2)(3\ 4)(2\ 3)(4\ 5)(3\ 4)(2\ 3)$  (このあたり授業ではやっていないかも知れません)

(5.17) の解答 (1) 互換の個数の偶奇は一定である (2) 奇置換

(5.18) の解答 それよりも、下の左図のあみだくじで、上の1, 2, ... から出発すると、下の1, 2, ... に到着するように横棒を引け、という問題が大事かも。その解答例は、下の右図。

