2021 年度 後期 代数学 1

担当 和地 輝仁

目次

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

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

§1 約数と倍数

(1.1) **整数** 整数全体の集合 $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ は無限集合である。最大値、最小値はない。加法、減法、乗法で閉じており、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、

$$a = bq + r \quad (0 \leq r < b) \tag{1}$$

を満たす整数 q, r が一意的に存在する。

Proof. [存在] a 割る b の商を q、余りを r とすれば、式 (1) を満たす。

ただし、a が負の場合の割り算ははっきりしないので、別証明も記しておく。正整数 b の倍数は、数直線上に b 間隔に存在する。数直線上で整数 a の左にあり、一番近い b の倍数を bq をとすると、b の倍数が b 間隔であることより、$0 \leq a - bq < b$ である。$r = a - bq$ と置けば、式 (1) を満たす。

[一意性] q と r が 2 通りに取れたとする。

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

このとき、これらより、$bq + r = bq' + r'$ だが、$r - r' = bq' - bq$ より $r - r'$ は b の倍数である。

また、r と r' の範囲より、$-b < r - r' < b$ である。$-b$ と b の間にある b の倍数は 0 のみだから、$r - r' = 0$ である。これより、$q = q'$ もわかり、r も q も一意的である。 □

(1.3) 倍数・約数・公倍数・公約数・最小公倍数・最大公約数

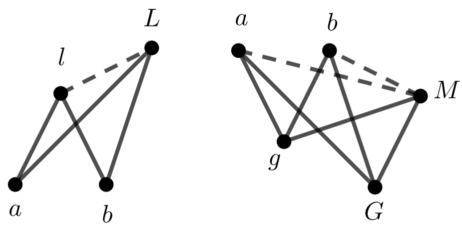
(1) 0 以上の整数 a, b が、$a = bt$ (t は整数) を満たしているとき、a を b の**倍数**、b を a の**約数**と呼ぶ。

(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。
例えば、$(8, 12) = 4$ である。

(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。



Proof. (1) a と b の公倍数 L があったとき、L を l で割って、

$$L = lq + r \quad (0 \leq r < l)$$

と表すと、$r = L - lq$ は再び a と b の公倍数である。ところが、r は最小公

倍数の l 未満なので、$r = 0$ である。つまり、$L = lq$ となり、L は l の倍数である。

(2) a と b の公約数 G があったとする。G と g の最小公倍数を M とする。M は g の倍数だから $M \geq g$ である。

さらに、M は a と b の公約数である。なぜなら、まず、a は G と g の公倍数だから (1) より a は M の倍数であり、次に、同様にして、b も M の倍数であるからである。

以上より、M は a と b の公約数であり、最小公倍数の g 以上であるから、$M = g$ である。M は G の倍数であるから、g は G の倍数である。 □

(1.5) **命題** a, b を 0 以上の整数で、少なくとも一方は 0 ではないとする。

(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。

Proof. (1) $g = (a, b)$ とする。$t = (\alpha, \beta)$ と置き、$\alpha = tx$, $\beta = ty$ $(x, y \in \mathbb{Z})$ と書く。すると、

$$a = g\alpha = gtx$$
$$b = g\beta = gty$$

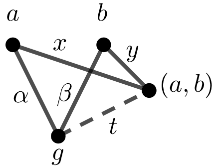
となり、gt が a と b の公約数になる。g の最小性から、$t = 1$、つまり、$(\alpha, \beta) = 1$ である。

逆に、$(\alpha, \beta) = 1$ とする。$a = (a, b)x$, $b = (a, b)y$ $(x, y \in \mathbb{Z})$ と書ける。また、g は a と b の公約数だから、最大公約数 (a, b) の約数なので、

$(a,b) = tg\ (t \in \mathbb{Z})$ と書ける。これらより、

$$a = (a,b)x = gtx$$
$$b = (a,b)y = gty$$

となる。$a = g\alpha,\ b = g\beta$ と比べると、t は α と β の公約数とわかるが、$(\alpha, \beta) = 1$ だったから $t = 1$ である。つまり、$g = (a,b)$ である。



(2) も同様。

(3) $a = g\alpha,\ b = g\beta$ と置くと、(1) より $(\alpha,\beta) = 1$ である。すると、

$$g\alpha\beta = a\beta$$
$$g\alpha\beta = b\alpha$$

となるので、$g\alpha\beta$ は a と b の公倍数であり、$(\alpha,\beta) = 1$ だから、(2) より、最小公倍数である。つまり、$l = g\alpha\beta$ である。

以上より、$gl = g \cdot g\alpha\beta = g\alpha \cdot g\beta = ab$ である。 □

(1.6) **問題** 上の命題の (2) を証明せよ。

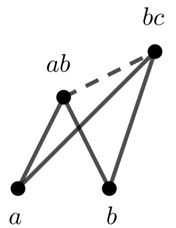
(1.7) **例** 12 と 8 の最大公約数、最小公倍数は、それぞれ、4 と 48 である。従って、$12 \cdot 8 = 4 \cdot 48$ が成立している。

(1.8)　**問題**　512 と 768 の最大公約数が 256 であることを用いて、最小公倍数を求めよ。

§2　素因数分解の一意性

(2.1)　**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。

Proof.



(1.5) (3) より a, b の最小公倍数は ab である。bc は a, b の公倍数だから (1.4)(1) より最小公倍数 ab の倍数である。つまり、bc は ab の倍数だから、b で割れば、c は a の倍数である。 □

(2.2)　**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。

(2.3) **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。

Proof. [存在] x を 2 以上の整数とする。x が 1 より大きく x より小さいどんな整数でも割り切れないならば、x は素数だから、x は素因数分解できていることになる。

割り切れたならば、$x = yz$ (y と z は x 未満の正整数) と分解でき、帰納法を用いると y も z も素因数分解できる ($y_1, \ldots, y_a$ と $z_1, \ldots, z_b$ は素数)。

$$y = y_1 y_2 \cdots y_a$$
$$z = z_1 z_2 \cdots z_b$$

辺々掛けた $x = yz = y_1 y_2 \cdots y_a \cdot z_1 z_2 \cdots z_b$ は x の素因数分解を与えるから、x も素因数分解できることがわかる。

[一意性] x を 2 以上の整数とする。x が 2 通りに素因数分解できたとする ($p_1, \ldots p_k$ と $q_1, \ldots q_l$ は素数)。

$$x = p_1 p_2 \cdots p_k$$
$$x = q_1 q_2 \cdots q_l$$

もしも、$p_1 = q_1$ だったら、素因数分解の先頭が一致していることがわかる。

もしも、$p_1 \neq q_1$ だったら、$q_1 q_2 \cdots q_l$ は p_1 で割り切れるので、(2.1) により、$q_2 \cdots q_l$ は p_1 で割り切れることがわかる。これを繰り返すと、p_1 は $q_2, \ldots, q_l$ のどれかと一致することになる。$q_1, q_2, \ldots, q_l$ の順番を交換すれば、$p_1 = q_1$ としてよく、やはり素因数分解の先頭が一致していることがわかる。

従って、$p_2 \cdots p_k = q_2 \cdots q_l$ となり、同じことを繰り返せば、先頭から順番に $p_i = q_i$ となっていくことがわかる。最後には、両方の素数をちょうど

使い切って $1 = 1$ になって終わるから、$k = l$ と、$p_i = q_i$ $(i = 1, 2, \ldots, k)$ がわかる。

つまり、素因数分解は素数の順番を除いて一意的である。 □

(2.4) **例** $\sqrt{2}$ は無理数であることを、素因数分解の一意性を用いて証明する。

途中までは、高校で学んだ背理法を用いた証明と同じである。$\sqrt{2}$ が有理数だと仮定すると、$\sqrt{2} = \frac{a}{b}$ (a と b は正整数) と書ける。両辺 2 乗して分母を払うと、$2b^2 = a^2$ となる。

(ここから違う) a と b の素因数分解を

$$a = p_1 p_2 \cdots p_k$$
$$b = q_1 q_2 \cdots q_l$$

とする。これを $2b^2 = a^2$ に代入すると、

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

となる。この両辺に現れる文字も「2」も素数であるから、両辺とも素因数分解されていることになる。ところが、左辺は奇数個、右辺は偶数個の素数の積なので、素因数分解の一意性に反する。よって、$\sqrt{2}$ は有理数ではない。

(2.5) **問題** $\sqrt{6}$ が無理数であることを証明せよ。【ヒント】$\sqrt{2}$ と同様に進めるが、最後、素数の個数で矛盾は出ない。「2」あるいは「3」の個数に着目して矛盾を出せばよい。

(2.6) **命題** 正整数 n が平方数ではないとき、$\sqrt{n}$ は無理数である。

Proof. 上に問題があるから、その解答になってしまわないよう、証明の概略のみ記す。

n が平方数ではないならば、その素因数分解を見たとき、奇数乗になっている素数 p が必ずある。上の問題と同様に証明を進めて、最後の所で、素数 p の個数に着目して矛盾を出せばよい。 □

(2.7) **エラトステネスのふるい** **エラトステネスのふるい**とは、ある範囲の素数を得る効率的な方法である。例えば 100 以下の素数を求める場合、次のようにする。

(A) 1 から 100 までの整数を書く。
(B) 1 を消す (素数ではないので)。
(C) この時点で消えていない最小の数は素数だから、丸を付ける。この数の 2 倍以上の倍数は素数ではないから消す。
(D) すべての数が消されるか、丸が付いたら終了。そうでなければ (C) に戻る。

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

(2.8) **問題** 100 までの素数は何個あるか。

(2.9) **定理** 素数は無数にある。

Proof. 有限個の素数 $p_1, p_2, \ldots, p_k$ があったとする。$x = p_1 p_2 \cdots p_k + 1$ は、これらのどの素数で割っても 1 余るので、割り切れない。従って、x の素因数分解には、$p_1, p_2, \ldots, p_k$ 以外の素数があるはずである。

このようにして次々に素数を生産できるので、素数は無数にある。 □

§3 1 次不定方程式

(3.1) **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。

Proof. (r, b) は r も b も割り切るから $a = bq + r$ も割り切る。よって、(r, b) は a と b の公約数であり、最大公約数の (a, b) 以下である。

同様にして、(a, b) は (r, b) 以下であることもわかる。合わせると、$(a, b) = (r, b)$ である。 □

(3.2) **問題** 上の証明の後半、(a, b) は (r, b) 以下であることを証明せよ。

(3.3) **問題** 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。

(3.4) **ベズーの等式** 高校でも学んだように、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。証明に代えて、次の例で解の求め方を示す。

(3.5) **例** $45x + 14y = 1$ のすべての整数解を求める。
(解答)

$$\begin{array}{rll} 45 \div 14 = 3 \text{ あまり } 3 & \text{より } 3 = 45 - 14 \cdot 3, & \text{(a)} \\ 14 \div 3 = 4 \text{ あまり } 2 & \text{より } 2 = 14 - 3 \cdot 4, & \text{(b)} \\ 3 \div 2 = 1 \text{ あまり } 1 & \text{より } 1 = 3 - 2, & \text{(c)} \end{array}$$

したがって、

$$\begin{aligned} 1 &\overset{\text{c}}{=} 3 - 2 \\ &\overset{\text{b}}{=} 3 - (14 - 3 \cdot 4) = 3 \cdot 5 - 14 \\ &\overset{\text{a}}{=} (45 - 14 \cdot 3) \cdot 5 - 14 = 45 \cdot 5 - 14 \cdot 16. \end{aligned}$$

よって、$(x, y) = (5, -16)$ がひとつの解である。

$45x + 14y = 1$ と $45 \cdot 5 + 14 \cdot (-16) = 1$ の辺々を引くと、$45(x - 5) + 14(y + 16) = 0$ となるが、45 と 14 は互いに素だから、$x - 5$ は 14 の倍数

である。$x-5=14k$ (k は定数) と置くと、

$$\begin{aligned} 45\cdot 14k+14(y+16)&=0,\\ 45k+(y+16)&=0,\\ y&=-16-45k. \end{aligned}$$

まとめると、$(x,y)=(5+14k,-16-45k)$ (k は整数)。

＊上の y の求め方に注意。$y+16$ が 45 の倍数だから $\cdots$ と x の場合と同じにしてはダメ。

(3.6) **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) $35x+13y=1$
(3) $35x-13y=2$
(4) $34x+24y=6$

§4 複素数

(4.1) **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 $(\pm\sqrt{a}i)^2=-a$ だから、$\pm\sqrt{a}i$ は**負数の平方根**である。つまり、

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

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**)。

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

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

(4.3) **問題** $(x+2yi)(1-2i)=7-9i$ のとき、実数 x, y を決定せよ。

(4.4) **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。実際、

$$z\bar{z}=(a+bi)(a-bi)a^2-(bi)^2=a^2+b^2$$
$$z+\bar{z}=(a+bi)+(a-bi)=2a$$

である。また、$\bar{z}=z$ ならば z は実数である。

(4.5) **問題** 複素数 z に対し、$\bar{z}=z$ ならば z は実数であることを示せ。

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

(4.7)　**問題**　分母を実数化し、$a+bi$ の形に書き直せ。
(1) $\dfrac{1}{2-3i}$　　(2) $\dfrac{2-5i}{3+4i}$

(4.8)　**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。

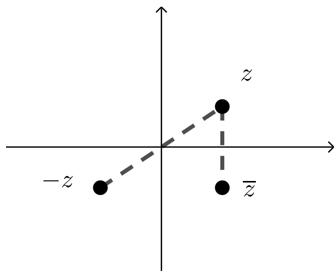
どちらも、当たり前に思えるが、(2) は、例えば行列に対しては成立しない性質である。

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

§5　複素数平面

(5.1)　**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、原点対称の位置に移動する。



(5.2) **絶対値** $z = a + bi$ のとき、複素数平面における点 z と原点との距離を $|z|$ と書き、z の**絶対値**と呼ぶ。三平方の定理より $|z| = \sqrt{a^2 + b^2}$ である。

実数の時の印象だと、「マイナスをプラスにする」ことと思ってしまうが、そうではないので注意する。つまり、$|1 - i| = 1 + i$ ではなく、$|1 - i| = \sqrt{2}$ である。

絶対値は次の性質を満たす。

(1) $|z|^2 = z\bar{z}$　　(2) $|-z| = |z|$　　(3) $|\bar{z}| = |z|$

(5.3) **問題** 上の 3 つの性質を証明せよ。(2) と (3) については、複素数の絶対値の定義を用いて、図形的に証明することが望ましい。

(5.4) **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。対応の様子を和についてだけ表にする。

ベクトル	ベクトルの和	和に対応する点
$\begin{pmatrix} a \\ b \end{pmatrix}$	$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ b+d \end{pmatrix}$	$(a+c, b+d)$

複素数	複素数の和	和に対応する点
$a+bi$	$(a+bi)+(c+di) = (a+c)+(b+d)i$	$(a+c, b+d)$

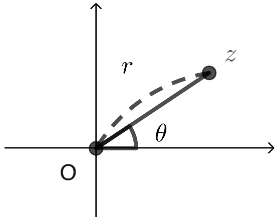
(5.5)　**実数倍の幾何的性質**　複素数 z と正の実数 k に対して、kz は z を原点中心に k 倍に拡大した点である。$-kz$ は $-z$ を原点中心に k 倍に拡大した点である。

実数 k に対して、$|kz| = |k||z|$ を満たす。

§6　極形式

(6.1)　**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 θ 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。θ が鋭角のときは、簡単な覚え方がある。

(6.2)　**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。



a

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。

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

cos と sin で違う角度を用いてはいけない。r に負の数を用いてはいけない。ダメばかりで嫌な感じであるが、そうとらえるよりは、絶対値 r と偏角 θ をまず求めるのが先決で、求めたら、上の式に代入するだけの穴埋め問題のようなものだと思えばよい。その先の式変形も一切しない。

唯一の例外として、$r = 1$ のときは、省略して $\cos\theta + i\sin\theta$ と表す。

(6.3) **例** $z = 1 + i$ は、絶対値が $\sqrt{2}$ で、偏角が 45° (あるいは $\frac{\pi}{4}$) なので、極形式は、

$$1 + i = \sqrt{2}(\cos 45^\circ + i\sin 45^\circ)$$

(の右辺) である。偏角の範囲に指定がなければ、45° の代わりに、405° や -315° 等を用いてもよい。

(6.4) **問題** 次の複素数を極形式で表せ。

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

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

【ヒント】$-z$ は -1 倍になったと思うと、r を $-r$ に変更してしまうが、絶対値の部分が負になってはいけない。基本に立ち返り、$-z$ の絶対値はいくらか、偏角はいくらかを図形的に考えればよい。$\bar{z}$ も同様に、絶対値と偏角がいくらかを図形的に考えればよい。

(6.6)　**問題 ($1/z$ の極形式)**　$z = r(\cos\theta + i\sin\theta)$ のとき、$\frac{1}{z}$ の極形式が、

$$\frac{1}{r}(\cos(-\theta) + i\sin(-\theta))$$

であることを示せ。

すなわち、**複素数の逆数において、絶対値は逆数に、偏角は -1 倍になる。**

【ヒント】残念ながら、図形的に考えるだけでは求められない。$\frac{1}{z}$ の分母を実数化することで、極形式に変形できる。

§7　複素数の乗除

(7.1)　**複素数の乗除**　三角関数の加法定理

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

を用いると、

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

のとき、

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

すなわち、**複素数の積において、絶対値は積に、偏角は和になる。**このことの証明は問題にあてる。

これを認めれば、商については、$\frac{z_1}{z_2} = z_1 \cdot \frac{1}{z_2}$ と思い、複素数の逆数において、絶対値は逆数になり、偏角は -1 倍になることを用いれば、**複素数の商において、絶対値は商に、偏角は差になる。**ことが直ちに証明できる。

(7.2) 問題

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

のとき、

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

を示せ。

(7.3) 複素数の乗除と絶対値

複素数 z, w に対して次が成り立つ。

(1) $|zw| = |z||w|, \quad \arg zw = \arg z + \arg w$

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

(7.4) **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 θ 回転し、r 倍に拡大した点である。

従って、絶対値が 1 である複素数 $z = \cos\theta + i\sin\theta$ を掛けることは、原点中心に θ 回転することにあたる。

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

(7.5) **問題 (乗除と幾何)**

(1) $2+i$ を原点の回りに 60° 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。

【ヒント】(2) は 3 通りの解があるので注意。

(7.6) **ド・モアブルの定理** 次の等式が成り立つ。

(1) $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta,$
(2) $\bigl(r(\cos\theta + i\sin\theta)\bigr)^n = r^n(\cos n\theta + i\sin n\theta)$

Proof. (1) がわかれば、指数法則を用いて (2) がわかるので、(1) のみ示す。まず、右辺は、複素数 1 を原点中心に $n\theta$ 回転した点である。

次に、左辺は、複素数 1 に対して、$\cos\theta + i\sin\theta$ を n 回掛けたものだから、複素数 1 を原点中心に角度 θ だけ回転することを n 回行った点である。これは、$n\theta$ 回転した点に他ならないから、左辺と右辺は等しい。 □

(7.7) 問題 $(1-i)^{12}$ を計算してみる。

$$\begin{aligned}(1-i)^{12} &= \left(\sqrt{2}(\cos(-\frac{\pi}{4}) + i\sin(-\frac{\pi}{4})\right)^{12} \\ &= (\sqrt{2})^{12}\left(\cos(-\frac{\pi}{4}\cdot 12) + i\sin(-\frac{\pi}{4}\cdot 12)\right) \\ &= 64\left(\cos(-3\pi) + i\sin(-3\pi)\right) \\ &= -64\end{aligned}$$

(7.8) 問題 計算して簡単にせよ。

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

§8 累乗根

この節では、特に断りがなければ、累乗根は複素数の範囲で考える。

(8.1) 命題 (n 乗根) n を正整数とする。複素数の範囲で、1 の n 乗根は、

$$\cos\left(\frac{k}{n}\times 360^\circ\right) + i\sin\left(\frac{k}{n}\times 360^\circ\right) \qquad (k = 0, 1, \ldots, n-1)$$

の n 個である。

Proof. $z^n = 1$ の解を複素数の範囲で求めればよい。z を極形式で表して、$z = r(\cos\theta + i\sin\theta)$ $(r > 0,\ \theta \in \mathbb{R})$ と置く。ド・モアブルの定理を用いると、$z^n = 1$ より、

$$r^n(\cos n\theta + i\sin n\theta) = 1$$

となる。両辺の絶対値と偏角を比較すると (右辺の 1 は、絶対値が 1、偏角は 0°)、偏角は 360° の整数倍異なっても同じ動径を表すことに注意すると、

$$\begin{cases} r = 1 \\ n\theta = 0^\circ + k \times 360^\circ \qquad (k \in \mathbb{Z}) \end{cases}$$

となる。従って、

$$z = \cos\theta + i\sin\theta$$

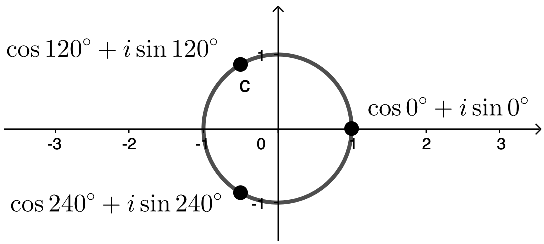
$$\text{ただし、}\theta = \frac{k}{n} \times 360^\circ \ (k \in \mathbb{Z})$$

である。

最後に、k がすべての整数を動くと、θ の表す動径に重複が起こるので、$0 \leq k < n$ に限定してよい。 □

(8.2) **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、$1, \dfrac{-1+\sqrt{3}i}{2}, \dfrac{-1-\sqrt{3}i}{2}$ の 3 つである。
この値自体よりも、複素数平面上の単位円周の 3 等分点であることが非常に重要である。



(2) 1 の 5 乗根は、単位円周上、1 から始めて 72° ごとに円周を 5 等分した点たちである。この、図形的な事実から、反対に、1 の 5 乗根は、

$\cos\theta + i\sin\theta$ $(\theta = 0°, 72°, 144°, 216°, 288°)$ だということもすぐわかる。ただし、その値は、$\sin 72°$ 等を知らなくては具体的には書けない。$\sin 72°$ は 2 重根号が必要な値である。

(8.3) **問題** 1 の 8 乗根を求めよ。

(8.4) **例 (1 ではない数の n 乗根)** 1 の n 乗根の求め方と同様にすると、1 ではない数の n 乗根も求められる。鍵になる考え方は、ド・モアブルの定理、あるいは、同じことだが、「複素数の積において、絶対値は積に、偏角は和になる」ことである。

例えば、2 の 4 乗根を求めてみる。$z^4 = 2$ とすると、z の絶対値は 4 乗すると 2 になる正の数だから、$\sqrt[4]{2}$ であり、z の偏角は、4 倍すると 360° や、360° の整数倍になるので、$\frac{k}{4} \times 360°$ $(k \in \mathbb{Z})$ であ ru. n 乗根はちょうど n 個ある事実を思い出せば、$k = 0, 1, 2, 3$ に限定してよい。

以上より、2 の 4 乗根は、

$$\sqrt[4]{2}(\cos\theta + i\sin\theta) \quad ただし、\theta = \frac{k}{4} \times 360° \quad (k = 0, 1, 2, 3)$$

である。つまり、$\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i$ の 4 つである。

(8.5) **問題** 8 の 3 乗根を求めよ。

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

(1) $1 + z + z^2 + \cdots + z^{n-1} = 0$

(2) $1 + \cos\theta + \cos 2\theta + \cdots + \cos(n-1)\theta = 0$

(3) $\sin\theta + \sin 2\theta + \cdots + \sin(n-1)\theta = 0$

【ヒント】(1) $z^n - 1 = 0$ だから、この左辺を因数分解してみよ。
(2) と (3) は、(1) において、ド・モアブルの定理を用いて、実部と虚部を比較せよ。

(8.7) **例** 三角形 ABC を考える。辺 CA、辺 AB、辺 BC の中点をそれぞれ X、Y、Z とする。三角形 ABC と三角形 XYZ は重心が一致し、さらに、相似であることを示せ。

Proof. 3 点 A, B, C を表す複素数を、それぞれ、a, b, c とする。必要であれば平行移動して、三角形 ABC の重心は原点であるとしてよい。このとき、$a + b + c = 0$ である。3 点 X, Y, Z を表す複素数を、それぞれ、x, y, z とすると、

$$x = \frac{b+c}{2}, \quad y = \frac{c+a}{2}, \quad z = \frac{a+b}{2}$$

であり、$a + b + c = 0$ を用いると、

$$x = -\frac{a}{2}, \quad y = -\frac{b}{2}, \quad z = -\frac{c}{2}$$

である。よって、三角形 XYZ の重心は、$\frac{x+y+z}{3} = -\frac{a+b+c}{6} = 0$ だから、三角形 ABC の重心と一致する。

また、x, y, z は、それぞれ、a, b, c を $-\frac{1}{2}$ 倍した数であるから、原点中心に 180 度回転して、原点中心に $\frac{1}{2}$ 倍に拡大したものである。従って、三角形 ABC と三角形 XYZ は相似である。相似比は 2 : 1 である。 □

(8.8) **問題 (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ことを示せ。

【ヒント】点 A, B, C を表す複素数を、それぞれ、a, b, c とし、偏角が 120 度である 1 の 3 乗根を ω とすると、辺 BC の上に立てた正三角形のもう 1 つの頂点は、$b+(b-c)\omega$ と表せる。このようにして、必要な頂点を、a, b, c, ω を用いて複素数で表すことから始める。

問題の 3 重心を頂点とする三角形は、その重心が三角形 ABC の重心と一致することがわかるから、$a+b+c=0$ とすれば計算が楽になる。正三角形の 3 頂点は、重心を中心として 120 度ずつ回転した位置にあるので、$a+b+c=0$ の下では、ω を順に掛けた複素数になっていることを示せばよい。

§9 群

(9.1) **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、$\boldsymbol{a^{-1}}$ と書く。

演算が「定義されている」というのは、G の元 a と b があったとき、演算の結果 $a \circ b$ が再び G に属することを言う。G は演算で**閉じている**とも

言う。

(9.2) 命題 (単位元、逆元の一意性)

(1) 結合法則があるので、3 つ以上の元の積も単に abc などと括弧なしに書いてよい。
(2) 単位元は一意的である。
(3) 逆元は一意的である。

Proof. (2) のみ示す。群 G の元 e, e' が、どちらも単位元の条件 (G2) を満たすとする。まず、e は単位元だから、$ee' = e'$ である。次に、e' は単位元だから、$ee' = e$ である。よって、$e = e'$ である。つまり、単位元は一意的である。 □

(9.3) 問題 上の命題の (3) を証明せよ。

【ヒント】(2) の証明のように、$x \in G$ に対して、$y, y' \in G$ がともに逆元の条件を満たす (例えば y ならば、$xy = yx = e$)) と仮定して、$y = y'$ を証明すればよい。

(9.4) 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** (**可換群**) 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。

(9.5) 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。$\mathbb{Q}^+$ は 0 以上の有理数全体の集合、$\mathbb{Q}^\times$ は 0 以外の有理数全体の集合、$\mathbb{R}^\times$ は 0 以外の実数全体の集合、$\mathbb{C}^\times$ は 0 以外の複素数全体の集合、$\mathbb{T}$ は絶対値が 1 である複素数全体の集合を表す。

(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。

Proof. 一部のみ証明する。

(1) $(\mathbb{Z}, +)$ について。整数と整数の和は、再び整数だから、$\mathbb{Z}$ は和で閉じている。(G1) 数の和なので結合法則は満たす。(G2) $0 \in \mathbb{Z}$ は単位元である。なぜなら、整数 a に対して、$a + 0 = 0 + a = a$ だからである (条件 (G2) では、演算が積で書かれているが、この問題では演算は和なので、このような条件に置きかわる)。(G3) $a \in \mathbb{Z}$ の逆元は $-a \in \mathbb{Z}$ である。なぜなら、$a + (-a) = (-a) + a = 0$ だからである (ここでも演算が積なのでこのような条件に置きかわる)。

(2) $(\mathbb{Q}^+, +)$ について。逆元で閉じていないので群ではない (例えば 1 の逆元は -1 だが、$\mathbb{Q}^+$ に属さない)。

(2) $(\mathbb{R}, \times)$ について。0 の逆元が存在しないので群ではない。

(4) $(\{1, -1\}, \times)$ について。± 1 どうしの積は、どの組合せでも ± 1 になるので、積で閉じている。(G1) 数の積なので結合法則を満たす。(G2) 1 は単位元である。(G3) 1 の逆元は 1、-1 の逆元は -1 なので、逆元で閉じている。 □

(9.6) **問題** 上の例の $(\mathbb{Q}^{\times}, \times)$ が群であることを示せ。また、$(\mathbb{T}, \times)$ が群であることを示せ。

【ヒント】$(\mathbb{T}, \times)$ について。$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ である。積で閉じていることを言うには、積が $\mathbb{T}$ に属すること、つまり、積の絶対値が 1 であることをを示せばよい。同様に、逆元で閉じていることを言うには、逆元の絶対値が 1 であることを示せばよい。

(9.7) **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。この項は、授業で図を見ないとわかりづらいと思います。

(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]

§10　部分群

(10.1)　**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。

(10.2)　**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。

(10.3)　**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。

(10.4) **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、$a^{-1}b \in H$.

Proof. [(i)⇒(ii)] H が G の部分群であるとする。任意の $a, b \in H$ をとったとき、群 H は演算で閉じているから $ab \in H$ であり、逆元でも閉じているから、$a^{-1} \in H$ である。

[(ii)⇒(iii)] 任意の $a, b \in H$ に対して、$ab \in H$ かつ $a^{-1} \in H$ を満たすとする。つまり、積と逆元で閉じているとする。このとき、$a^{-1} \in H$ だから、H の元どうしの積 $a^{-1}b$ も H の元である。

[(iii)⇒(i)] 任意の $a, b \in H$ に対して、$a^{-1}b \in H$ を満たすとする。$a = b$ とすると $a^{-1}a = e \in H$ となるから、(G2) を満たす。$e \in H$ がわかったので、$b = e$ とすると、$a^{-1}e = a^{-1} \in H$ となるから、(G3) を満たす。H は G の部分集合なので、(G1) 結合法則は満たす。$a, b \in H$ に対して、$a^{-1} \in H$ であることはわかったので、$(a^{-1})^{-1}b = ab \in H$ となり、積で閉じていることがわかる。以上より、H は部分群である。 □

(10.5) **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。

【ヒント】上の定理の条件 (ii) (や (iii)) を用いるとよい。

§11　対称群

(11.1)　**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 Ω と置く。全単射 $\sigma : \Omega \to \Omega$ を n 文字の**置換**と呼ぶ。置換 σ が、1 を i_1 に, 2 を i_2 に, ..., n を i_n に写すとき、

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

と書く。例えば、1 を 2 に、2 を 4 に、3 を 3 に、4 を 1 に写す 4 文字の置換では、

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

となる。

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

$$(\sigma\tau)(i) = \sigma(\tau(i)) \qquad (i = 1, 2, \ldots, n)$$

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

(11.2) **例** (S_3) 3 次対称群 S_3 は、

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

であり、積の一例は、

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

であり、逆元の一例は、

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

である。

(11.3)　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 (あるいは id) 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。

(11.4)　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。

(11.5)　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 $i_1, i_2, \ldots, i_k$ 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、$\ldots$, 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。

(11.6)　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 (2) 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 (2) のように表示せよ。

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

(11.8)　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、σ^2 と σ^{-1} を求めよ。
(2) 長さ k の巡回置換 σ に対して、σ^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 σ に対して、σ^2 が再び巡回置換になるための条件を求めよ。

(11.9) 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、

$$\begin{aligned}(\,a\ b\,) = (\,a\ a+1\,)(\,a+1\ a+2\,)\cdots(\,b-2\ b-1\,)\cdot(\,b-1\ b\,)\\ \cdot(\,b-2\ b-1\,)(\,b-3\ b-2\,)\cdots(\,a\ a+1\,)\end{aligned}$$

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、$\{1, 2, \ldots, n\}$ のうち 1 つの数をとり i_1 とする。$i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, $\ldots$ 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、τ_1 と τ_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。 □

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。

(11.10) **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。

§12 偶置換・奇置換

(12.1) **定義 (転倒数)** 順列 $i_1, i_2, \ldots, i_n$ 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 $i_1, i_2, \ldots, i_n$ 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。

(12.2) **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 σ^{-1} の転倒数は等しいことを示せ。
(3) S_5 で転倒数が最大の元は何か。

(12.3) **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、σ 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、σ 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) $\sigma = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)$ とすると、

$$\sigma\tau = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)(\, a \;\, a+1\,) = \left(\begin{smallmatrix} 1 & \cdots & a & a+1 & \cdots & n \\ i_1 & \cdots & i_{a+1} & i_a & \cdots & i_n \end{smallmatrix}\right)$$

である。σ 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 σ 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。 □

(12.4) **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。

(12.5) **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。

(12.6)　**定理**　$\sigma \in S_n$ を隣接互換の積で表す最小個数は、σ 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 σ の転倒数だけ必要であることは、(12.3) 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。$\sigma = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)$ 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、σ 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 σ の転倒数である。従って、$\sigma = \tau_k\cdots\tau_2\tau_1$ と σ を転倒数の個数の隣接互換の積で表せた。 □

(12.7)　**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。(11.9) 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引かれる横棒だけで実現できる。(12.3) 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。(12.6) 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。

(12.8)　**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。

(12.9) **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、$\boldsymbol{n}$ **次交代群**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。

(12.10) **定義** $^{\#}$ ($\operatorname{sgn}\sigma$) 置換 σ に対して、

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

で定める $\operatorname{sgn}(\sigma)$ を、置換 σ の**符号**と呼ぶ。

§13 準同型

(13.1)　定義 (準同型写像)　群 G から群 H への写像 $f : G \to H$ が、次の 2 条件を満たすとき、f を群の**準同型** (**準同型写像**) と呼ぶ。

(H) $f(ab) = f(a)f(b)$ $(a, b \in G)$

　このとき、

(1) $f(e) = e$
(2) $f(a^{-1}) = f(a)^{-1} \quad (a \in G)$

が成り立つ。

(13.2)　例　実数全体の集合 $\mathbb{R}$ や整数全体の集合 $\mathbb{Z}$ は和に関して群であり、正の実数全体の集合 $\mathbb{R}^+$ や、0 ではない実数全体の集合 $\mathbb{R}^\times$ は、積に関して群である。

(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = 2x)$ は群の準同型である。

(2) $f : \mathbb{Z} \to \mathbb{Z}$ $(f(x) = -x)$ は群の準同型である。

(3) $f : \mathbb{R}^+ \to \mathbb{R}^+$ $(f(x) = x^2)$ は群の準同型である。

(4) $f : \mathbb{R}^\times \to \mathbb{R}^+$ $(f(x) = x^2)$ は群の準同型である。

(5) $f : \mathbb{R} \to \mathbb{R}^+$ $(f(x) = 2^x)$ は群の準同型である。

(6) S_n を n 次対称群、$G = \{1, -1\}$ を積に関する群とするとき、符号 $\mathrm{sgn} : S_n \to G$ は群の準同型である。

(13.3)　定義 (同型写像)　群 G から群 H への準同型写像 $f : G \to H$ が、全単射であるとき、f を群の**同型** (**同型写像**) と呼ぶ。

(13.4) **例** 実数全体の集合 $\mathbb{R}$ や整数全体の集合 $\mathbb{Z}$ は和に関して群であり、正の実数全体の集合 $\mathbb{R}^+$ や、0 ではない実数全体の集合 $\mathbb{R}^\times$ は、積に関して群である。

(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = 2x)$ は群の同型である。

(2) $f : \mathbb{Z} \to \mathbb{Z}$ $(f(x) = 2x)$ は群の同型ではない。

(3) $f : \mathbb{R}^+ \to \mathbb{R}^+$ $(f(x) = x^2)$ は群の同型である。

(4) $f : \mathbb{R}^\times \to \mathbb{R}^+$ $(f(x) = x^2)$ は群の同型ではない。

(5) $f : \mathbb{R} \to \mathbb{R}^+$ $(f(x) = 2^x)$ は群の同型である。

(6) n 次対称群 S_n の符号 $\mathrm{sgn} : S_n \to \{1, -1\}$ は群の同型ではない。

(13.5) **定義 (群の同型)** 群 G から群 H への同型写像があるとき G と H は**同型**であると言い、$G \simeq H$ と書く。群が同型であるとは「乗積表」が一致することを意味する。

(13.6) **例** G を正方形ではない長方形の合同変換群とする。つまり、

$$G = \{\mathrm{id}, \sigma, \tau, \rho\}$$

id は恒等変換
σ は水平な対称軸を持つ対称移動の変換
τ は鉛直な対称軸を持つ対称移動の変換
ρ は 180 度回転移動の変換

とする。また、行列の積を演算とする群 H を次で定める。

$$H = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\}$$

このとき、次で定まる写像 $f : G \to H$ は群の同型であり、G と H は同型である。

$$f(\mathrm{id}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad f(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \quad f(\tau) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad f(\rho) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$$

G と H の乗積表は下のようになっており、ちょうど対応することが確認できる。

G	id	σ	τ	ρ
id	id	σ	τ	ρ
σ	σ	id	ρ	τ
τ	τ	ρ	id	σ
ρ	ρ	τ	σ	id

H	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(13.7)　**問題**　実数全体の集合 $\mathbb{R}$ は和に関して群であり、正の実数全体の集合 $\mathbb{R}^+$ は積に関して群である。次の同型写像について、逆写像を求め、それらも同型写像であることを示せ。

(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = 2x)$

(2) $f : \mathbb{R}^+ \to \mathbb{R}^+$ $(f(x) = x^2)$

(3) $f : \mathbb{R} \to \mathbb{R}^+$ $(f(x) = 2^x)$

(13.8)　**問題**　群の準同型写像 $f : G_1 \to G_2$ と $g : G_2 \to G_3$ があるとする。

(1) 合成写像 $g \circ f$ も準同型であることを示せ。

(2) f も g も同型ならば、合成写像 $g \circ f$ も同型であることを示せ。

§14　演習問題

(14.1)　**問題**　素数の定義を言え。

(14.2)　**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。

(14.3) **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) $448, 588$

(14.4) **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) $39x - 11y = -3$

(14.5) **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) $\dfrac{1+i}{2-i}$

(14.6) **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 α, β $(\alpha \leq \beta)$ と置くと、解と係数の関係より、$\alpha\beta = 1$ である。」

(14.7) **問題** 複素数 $z = 2 - i$ に対して次を求めよ。

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

(14.8) **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) $-\sqrt{2}+\sqrt{2}i$

(14.9) **問題** 次の問に答えよ。

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

(14.10) **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) $(1-i)^9$

(14.11) **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。

(14.12) **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) $(\mathbb{C}^\times,\times)$

(14.13) **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

(14.14) **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、$0°$, $120°$, $240°$ 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。

(14.15) **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。

(14.16) **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。

(14.17) **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。

(14.18) **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。

```
| | | | |
| |-| | |
| | |-| |
| | | |-|
| | |-| |
| |-| | |
|-| | | |
| |-| | |
| | |-| |
| | | |-|
| | |-| |
| |-| | |
```

|-| | | |
| | | | |

以下は、過去に期末試験で出題された問題の一部である。

(14.19) **問題 (2014)** 次の問に答えよ。

(1) 8352 と 7632 の最大公約数を答えよ。

(2) 8352 と 7632 の公約数の個数を答えよ。

(3) 8352 と 7632 の公約数のうち、小さい方から 5 番目のものを答えよ。

(14.20) **問題 (2014)** 無限小数の値をどう定めるかの定義を書け。また、それに基いて無限小数 $0.999\cdots$ が 1 に等しいことを証明せよ。

(14.21) **問題 (2014)** $\sqrt[3]{2}$ が無理数であることを次のように証明したが、誤りがある。どこが誤りか指摘せよ。

(証明) 正整数 a, b を用いて、$\sqrt[3]{2} = \dfrac{a}{b}$ と書けたと仮定する。両辺を 3 乗して分母を払うと、$2b^3 = a^3$ を得る。a と b の素因数分解を

$$a = p_1 p_2 \cdots p_s, \qquad b = q_1 q_2 \cdots q_s$$

(p_i, q_j は素数。重複も許す) と書き、上の式に代入すると、

$$2 \cdot q_1^3 q_2^3 \cdots q_s^3 = p_1^3 p_2^3 \cdots p_s^3$$

となり、両辺で掛け合わされている素数の個数が一致しないので、素因数分解の一意性に矛盾。よって、仮定が誤りであり $\sqrt[3]{2}$ は無理数である。(証明終)

(14.22) **問題 (2014)** 方程式 $34x-24y=6$ の整数解を 1 組求めよ。

(14.23) **問題 (2014)** 次の計算をし、簡単にせよ。ただし、i は虚数単位を表す。

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

(14.24) **問題 (2014)** 4 つの複素数 $z_1=2, z_2=-3, z_3=4i, z_4=5+4i$ について次の問に答えよ。

(1) 2 点 z_1, z_3 を結ぶ線分と、2 点 z_2, z_4 を結ぶ線分が直交することを示せ。

(2) 4 点 z_1, z_2, z_3, z_4 はひし形の 4 頂点をなすこと示せ。

(14.25) **問題 (2014)** 次の問に答えよ。

(1) $z=\sqrt{3}+3i$ を極形式に直せ。

(2) $(\sqrt{3}+3i)^9$ を計算し、$a+bi$ の形で答えよ。

(14.26) **問題 (2014)** $\zeta\in\mathbb{C}$ を 1 の 8 乗根であって偏角が 45° であるものとし、k を整数とする。

(1) ζ^k の絶対値を求めよ。

(2) ζ^k が 1 の 8 乗根であることを示せ。

(14.27)　**問題 (2014)**　$\mathbb{C}$ の部分集合 $\mathbb{T}$ を次で定めるとき、$\mathbb{T}$ が乗法に関して群をなすことを示せ。　$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$

(14.28)　**問題 (2014)**　正方形の合同変換の個数を答えよ。ただし、合同変換には、鏡に映したように裏表が反転するものも含める。

(14.29)　**問題 (2014)**　5 次対称群 S_5 の元 σ, τ を次で定めるとき、次の問に答えよ。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$$

(1) 積 $\sigma\tau$ を計算せよ。

(2) σ の逆元を答えよ。

(3) σ を隣接互換の積で表せ。

(4) σ を隣接互換の積で表すときの最小個数を求めよ。

§15　問題の解答

(1.8) の解答　a と b の最大公約数と最小公倍数を、それぞれ、g と l とすると、$ab = gl$ なので、$a = 512, b = 768$ のとき、$512 \cdot 768 = 256l$ である。これより、$l = 1536$ である。

(3.6) の解答　$(1)5, 16$ $(2)3, -8$ $(3)6, 16$ $(4)15, -21$

(14.1) 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。

(14.2) 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。$a = p_1p_2\cdots p_k$, $b = q_1q_2\cdots q_l$ 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、

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

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。

(14.3) 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.

(14.4) の解答　(1)

$$\begin{aligned}
39 \div 28 &= 1 \text{ あまり } 11 & &\text{より } 11 = 39 - 28, & &\text{(a)}\\
28 \div 11 &= 2 \text{ あまり } 6 & &\text{より } 6 = 28 - 11 \cdot 2, & &\text{(b)}\\
11 \div 6 &= 1 \text{ あまり } 5 & &\text{より } 5 = 11 - 6, & &\text{(c)}\\
6 \div 5 &= 1 \text{ あまり } 1 & &\text{より } 1 = 6 - 5. & &\text{(d)}
\end{aligned}$$

したがって、

$$\begin{aligned}
1 &\overset{\mathrm{d}}{=} 6 - 5\\
&\overset{\mathrm{c}}{=} 6 - (11 - 6) = 6 \cdot 2 - 11\\
&\overset{\mathrm{b}}{=} (28 - 11 \cdot 2) \cdot 2 - 11 = 28 \cdot 2 - 11 \cdot 5\\
&\overset{\mathrm{a}}{=} 28 \cdot 2 - (39 - 28) \cdot 5 = 28 \cdot 7 - 39 \cdot 5.
\end{aligned}$$

よって、$(x, y) = (-5, 7)$.

(2)

$$\begin{aligned}
28 \div 11 &= 2 \text{ あまり } 6 & &\text{より } 6 = 28 - 11 \cdot 2, & &\text{(a)}\\
11 \div 6 &= 1 \text{ あまり } 5 & &\text{より } 5 = 11 - 6, & &\text{(b)}\\
6 \div 5 &= 1 \text{ あまり } 1 & &\text{より } 1 = 6 - 5. & &\text{(c)}
\end{aligned}$$

したがって、

$$\begin{aligned} 1 &\overset{\mathrm{c}}{=} 6-5 \\ &\overset{\mathrm{b}}{=} 6-(11-6) = 6\cdot 2 - 11 \\ &\overset{\mathrm{a}}{=} (28-11\cdot 2)\cdot 2 - 11 = 28\cdot 2 - 11\cdot 5. \end{aligned}$$

よって、$(x,y)=(2,5)$.

(3)

$$\begin{aligned} 39 \div 11 &= 3 \text{ あまり } 6 \qquad & &\text{より } 6 = 39 - 11\cdot 3, & \text{(a)} \\ 11 \div 6 &= 1 \text{ あまり } 5 & &\text{より } 5 = 11 - 6, & \text{(b)} \\ 6 \div 5 &= 1 \text{ あまり } 1 & &\text{より } 1 = 6 - 5. & \text{(c)} \end{aligned}$$

したがって、

$$\begin{aligned} 1 &\overset{\mathrm{c}}{=} 6-5 \\ &\overset{\mathrm{b}}{=} 6-(11-6) = 6\cdot 2 - 11 \\ &\overset{\mathrm{a}}{=} (39-11\cdot 3)\cdot 2 - 11 = 39\cdot 2 - 11\cdot 7. \end{aligned}$$

よって、両辺 -3 倍すると、$(x,y)=(-6,-21)$ がわかる。

(14.5) の解答　(1) $-1+2i$　(2) $3+i$　(3) $\dfrac{1+3i}{5}$

(14.6) 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。

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

(14.8) 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) $2(\cos 135^\circ + i\sin 135^\circ)$

(14.9) 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 $\frac{\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i$).

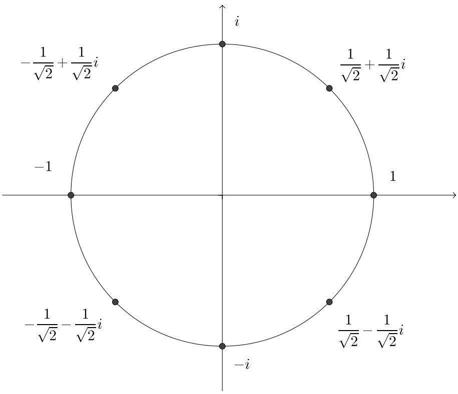
(14.10) の解答　(1)

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

(2)

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

(14.11) の解答　(1) 1 の 8 乗根は $\cos\theta + i\sin\theta$ ($\theta = \frac{360^\circ}{8}\times k,\ k = 0,1,\ldots,7$) だから、$\theta = 45^\circ \times k$ ($k=0,1,\ldots,7$) 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) $\cos\theta + i\sin\theta$ $(\theta = 0^\circ, 72^\circ, 144^\circ, 216^\circ, 288^\circ)$.

(14.12) の解答　(1) (9.1) を見よ。(2) すべて群である。

(14.13) 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。

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

(14.15) の解答　(1) (11.1) 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) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

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

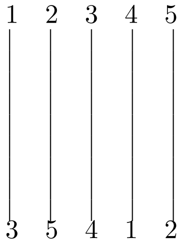
(2) (1) から続けて、$(\,1\ 3\,)(\,3\ 4\,)(\,2\ 5\,) = (\,1\ 2\,)(\,2\ 3\,)(\,1\ 2\,)\cdot(\,3\ 4\,)\cdot(\,2\ 3\,)(\,3\ 4\,)(\,4\ 5\,)(\,3\ 4\,)(\,2\ 3\,)$.

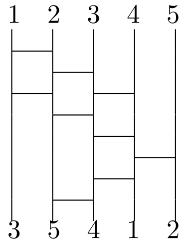
(3) 7 (このあたり授業ではやっていないかも知れません)

(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)

(14.17) の解答　(1) 互換の個数の偶奇は一定である　(2) 奇置換

(14.18) の解答　それよりも、下の左図のあみだくじで、上の $1, 2, \ldots$ から出発すると、下の $1, 2, \ldots$ 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。





(14.19) の解答　(1) 例えばユークリッドの互除法で求めると、144.
(2) 144 の約数の個数だから、$144 = 2^4 \cdot 3^2$ より、個数は $5 \times 3 = 15$ 個。
(3) 144 の約数のうち、小さい方から 5 番目のものだから、6.

(14.20) の解答　小数部分が、$0.a_1a_2a_3\cdots$ (a_j は小数第 j 位の数字) であるとき、その値は無限級数

$$\frac{a_1}{10^1}+\frac{a_2}{10^2}+\frac{a_3}{10^3}+\cdots=\sum_{j=1}^{\infty}\frac{a_j}{10^j}$$

で定まる。整数部分があるときは、これに加える。

この定義に基づくと、無限等比級数の和の公式より、

$$0.999\cdots=\frac{9}{10^1}+\frac{9}{10^2}+\frac{9}{10^3}+\cdots=\frac{\frac{9}{10}}{1-\frac{1}{10}}=\frac{\frac{9}{10}}{\frac{9}{10}}=1$$

である。

(14.21) の解答　$a = p_1p_2\cdots p_s$, $b = q_1q_2\cdots q_s$ と、共に同じ s 個の素数の積で表した所が誤り。正しくは s 個と t 個のように、別の個数にすべき。

(14.22) の解答　両辺 2 で割り、$17x - 12y = 3$ を解けばよい。

$$\begin{aligned}
17 \div 12 &= 1 \text{ あまり } 5 && \text{より } 5 = 17 - 12, && \text{(a)}\\
12 \div 5 &= 2 \text{ あまり } 2 && \text{より } 2 = 12 - 5\cdot 2, && \text{(b)}\\
5 \div 2 &= 2 \text{ あまり } 1 && \text{より } 1 = 5 - 2\cdot 2, && \text{(c)}
\end{aligned}$$

したがって、

$$\begin{aligned}1 &\overset{\mathrm{c}}{=} 5-2\cdot 2\\ &\overset{\mathrm{b}}{=} 5-(12-5\cdot 2)\cdot 2 = 5\cdot 5-12\cdot 2\\ &\overset{\mathrm{a}}{=} (17-12)\cdot 5-12\cdot 2 = 17\cdot 5-12\cdot 7.\end{aligned}$$

よって、$17\cdot 5-12\cdot 7=1$ だが、両辺 3 倍すると、 $17\cdot 15-12\cdot 21=3$ となるから、$(x,y)=(15,21)$.

(14.23) の解答　(1) $1+7i$　 (2) $\sqrt{2}$

(14.24) の解答　(1) $z_3-z_1=4i-2,\ z_4-z_2=4i+8$ であるから、$z_4-z_2=-2i(z_3-z_1)$ である。つまり、z_1, z_3 を結ぶ線分を、$-\pi/2$ 回転して長さを 2 倍したものが z_2, z_4 を結ぶ線分であり、特に 2 つの線分は直交する。

(2) $z_1-z_2=5$, $z_4-z_3=5$ だから、1 組の対辺が平行で長さが等しいから平行四辺形である。対角線が直交する平行四辺形だからひし形である。

((2) 別解) 4 辺の長さが等しいことを複素数平面で、あるいは、xy 平面で確かめてもよい。

(14.25) の解答　(1) $2\sqrt{3}(\cos 60^\circ+i\sin 60^\circ)$

(2) $(\sqrt{3}+3i)^9 = \left(2\sqrt{3}(\cos 60^\circ+i\sin 60^\circ)\right)^9 = (2\sqrt{3})^9(\cos 540^\circ + i\sin 540^\circ) = 41472\sqrt{3}\cdot(-1) = -41472\sqrt{3}$

(14.26) の解答　(1) $|\zeta^k|=|\zeta|^k=1^k=1$

(2) $(\zeta^k)^8=\zeta^{8k}=(\zeta^8)^k=1^k=1$ である。ζ^k は 8 乗して 1 になるので、1 の 8 乗根である。

(別解 (出題者の意図ではまったくない)) $\zeta=\cos(\pi/8)+i\sin(\pi/8)$ だから、$\zeta^k=\cos(k\pi/8)+i\sin(k\pi/8)$ である。この極形式を見ると絶対値は 1

であり、1 の 8 乗根である。

(14.27) の解答　まず、積で閉じていることを示す。$z, w \in \mathbb{T}$ をとると、$|zw| = |z||w| = 1 \cdot 1 = 1$ となり、$zw \in \mathbb{T}$ である。

結合法則の成立は明らか。

次に、1 は (絶対値が 1 だから) $\mathbb{T}$ に属する。つまり単位元が存在する。

最後に、$z \in \mathbb{T}$ のとき、$|z^{-1}| = |z|^{-1} = 1^{-1} = 1$ となり、$z^{-1} \in \mathbb{T}$ である。つまり、逆元も $\mathbb{T}$ に属する。

以上より、$\mathbb{T}$ は乗法に関して群である。

(14.28) の解答　1 つの頂点の移る先が 4 通り、その隣の頂点の移る先が 2 通りである。この 2 点が決まれば残りの 2 点の移る先も決まるので、$4 \times 2 = 8$ 個。

(14.29) の解答　(1) $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{smallmatrix}\right)$

(2) $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{smallmatrix}\right)$

(3) $\sigma = \left(\begin{smallmatrix} 1 & 4 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 3 & 5 \end{smallmatrix}\right) = (14)(24) \cdot (35) = (12)(23)(34)(23)(12) \cdot (23)(34)(23) \cdot (34)(45)(34)$

((3) 別解) 最小個数で答えて、例えば、$(34)(45)(23)(34)(12)$ でもよい。

(4) 最小個数は σ の転倒数に等しいから、5 個。