1の n 乗根と原始 n 乗根

発展　高2数学・複素数平面

絶対値が 1 の複素数をかけると、複素数平面の点は原点のまわりにその偏角だけ回ります。この頁ではこの見方を足場にして、方程式 $z^n = 1$ の解を調べます。§1〜§3 は授業で扱った問題の背景にあたる内容で、§4 は同じ論法を整数の余りに当てはめた話、§5 は入試に出たことのある発展的な話題です。

1. $z^n = 1$ の解は正 n 角形の頂点に並ぶ

$z = r(\cos\theta + i\sin\theta)$ $(r > 0)$ とおくと、ド・モアブルの定理から $z^n = r^n(\cos n\theta + i\sin n\theta)$ です。これが 1 に等しくなるのは、$r^n = 1$ で、しかも $n\theta$ が 2π の整数倍のときです。よって $r = 1$、$\theta = \dfrac{2\pi k}{n}$（$k$ は整数）となります。k を n だけ増やすと偏角が 2π 増えて同じ点に戻るので、異なる解は

$$\xi_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \qquad (k = 0,\ 1,\ \dots,\ n-1)$$

の n 個です。これらを **1 の n 乗根**と呼びます。偏角が $\dfrac{2\pi}{n}$ ずつ増えるので、n 個の点は単位円を n 等分し、1 を頂点の一つとする正 n 角形の頂点になります。なお $\xi_n = \xi_0 = 1$ なので、番号を 1 から n まで振っても同じ n 個を表します（§2 ではそちらを使います）。

一つの 1 の n 乗根 z をとって $1,\ z,\ z^2,\ \dots$ と並べるとき、隣の頂点へ一つずつ進むとは限りません。z をかけるたびに点は z の偏角だけ回るので、z の偏角が大きければ一度に何個も頂点を飛ばします。図1は $n = 7$、$z = \xi_3$（偏角は $\dfrac{3}{7}\cdot 2\pi$）の場合で、$1 \to z \to z^2 \to \cdots \to z^7 = 1$ と結ぶと、星形を描きながら単位円を 3 周して、7 個の頂点をちょうど 1 回ずつ通ります。

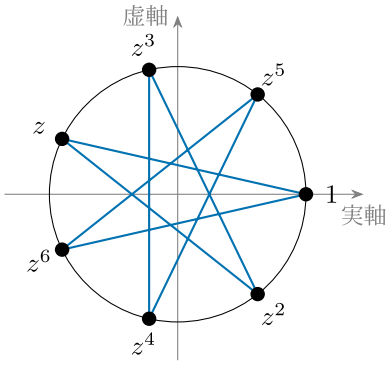


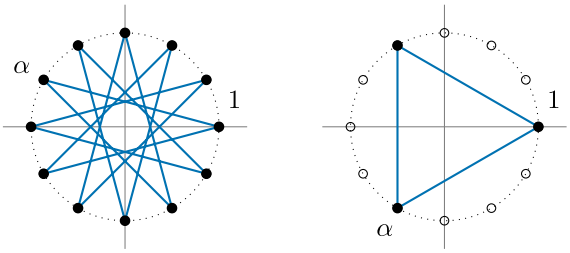
図1　1 の 7 乗根と、z の偏角が $\frac{3}{7}$ 周のときの $1,\ z,\ z^2,\ \dots,\ z^6$ の位置。順に結ぶと星形になる

授業で扱った問題のように「$1,\ z,\ z^2,\ \dots,\ z^{n-1}$ が正 n 角形の頂点をなす」という場面でも、この順に隣り合っているかどうかは別に確かめる必要があります。

2. はじめて 1 に戻る回数と原始 n 乗根

図1の z は 7 回かけてはじめて 1 に戻りました。ところが、どの 1 の n 乗根でも n 回かかるわけではありません。$n=12$ で偏角 $\dfrac{8}{12}\cdot 2\pi=\dfrac{4\pi}{3}$ の点 α をとると、α^3 の偏角は 4π なので $\alpha^3=1$ となり、α のべきは 12 個の頂点のうち 3 個しか通りません（図2の右）。この違いを言葉にするために、次の用語を使います。

> **位数と原始 n 乗根**
>
> 複素数 z について、$z^k=1$ を満たす最小の正の整数 k を z の**位数**という。
>
> 1 の n 乗根のうち、位数がちょうど n であるもの（n 乗して**はじめて** 1 になるもの）を 1 **の原始 n 乗根**という。



α の偏角 $\frac{5}{12}\cdot 2\pi$（位数 12）　　α の偏角 $\frac{8}{12}\cdot 2\pi$（位数 3）

図2　1 の 12 乗根。左は偏角 $\frac{5}{12}$ 周の α のべきが 12 個すべてを通る様子、右は偏角 $\frac{8}{12}$ 周の α のべきが 3 個だけを通る様子

$n=12$ について、ξ_m（偏角 $\dfrac{m}{12}\cdot 2\pi$）の位数を $m=1,\dots,12$ で全部書き出すと次の表になります。

m	位数	m	位数
1	12	7	12
2	6	8	3
3	4	9	4
4	3	10	6
5	12	11	12
6	2	12	1

表の位数は、分数 $\dfrac{m}{12}$ を約分しきったときの分母になっています。たとえば $\dfrac{8}{12}=\dfrac{2}{3}$ なので位数は 3、$\dfrac{9}{12}=\dfrac{3}{4}$ なので位数は 4 です。約分できない $m=1,5,7,11$ だけが位数 12、すなわち原始 12 乗根です。一般に次が成り立ちます。

> **ξ_m の位数と、原始 n 乗根になる条件**

$\xi_m = \cos\dfrac{2\pi m}{n} + i\sin\dfrac{2\pi m}{n}$ $(m = 1, 2, \ldots, n)$ について、m と n の最大公約数を d とすると

$$\xi_m \text{ の位数} = \frac{n}{d}$$

特に、ξ_m が 1 の原始 n 乗根であるのは、m と n が互いに素のとき、かつそのときに限る。

証明

正の整数 k について、$\xi_m^k = \cos\dfrac{2\pi mk}{n} + i\sin\dfrac{2\pi mk}{n}$ が 1 になるのは、$\dfrac{mk}{n}$ が整数のとき、つまり n が mk を割り切るときである。$m = dm'$、$n = dn'$ とおくと m' と n' は互いに素で、「n が mk を割り切る」は「n' が $m'k$ を割り切る」と同じである。n' は m' と共通の素因数を持たないので、これは「n' が k を割り切る」と同値になる。そのような正の整数 k のうち最小のものは $k = n' = \dfrac{n}{d}$ である。 □

1 の原始 n 乗根の個数は、1 以上 n 以下で n と互いに素な整数の個数に等しくなります。$n = 12$ なら 4 個、n が素数 p なら 1 以外の $p - 1$ 個すべてです。

3. 原始 n 乗根のべきは n 乗根をすべて出す

図2の左では、原始 12 乗根 α のべき $\alpha, \alpha^2, \ldots, \alpha^{12}$ が 12 個の頂点を 1 回ずつ通っていました。これは偶然ではありません。

原始 n 乗根のべき

α を 1 の原始 n 乗根とすると、$\alpha, \alpha^2, \ldots, \alpha^n$ は互いに異なり、この n 個で 1 の n 乗根がすべて出そろう。

証明

各 α^k は $(\alpha^k)^n = (\alpha^n)^k = 1$ を満たすので 1 の n 乗根である。1 の n 乗根は全部で n 個しかないから、$\alpha, \ldots, \alpha^n$ が互いに異なることさえ言えれば、n 個すべてが現れる。

$\alpha^k = \alpha^l$ $(1 \leqq k < l \leqq n)$ となる組があったとする。$\alpha \neq 0$ なので両辺を α^k で割れて、$\alpha^{l-k} = 1$ となる。ところが $1 \leqq l - k \leqq n - 1$ であり、これは α の位数が n であることに反する。よって $\alpha, \ldots, \alpha^n$ は互いに異なる。 □

逆に、α の位数 e が n より小さいと、$\alpha^{k+e} = \alpha^k$ なので同じ点が e 個ごとにくり返し現れ、べきが通る点は e 個だけです（図2の右は $e = 3$）。

証明の中身は「二つが重なったと仮定すると、その差の回数だけかけて 1 に戻ることになり、位数より少ない回数で戻るので矛盾」という一行です。次の §4 と §5 でも、この形の議論をもう一度使います。

4. 同じ論法を整数の余りに使う

1 の n 乗根の世界の「α をかけて回る」を、整数の世界の「a を足して b で割った余りを見る」に置き換えると、ほとんど同じ議論が通ります。$a=5$、$b=7$ で $5, 10, 15, 20, 25, 30$ を 7 で割った余りを並べると $5, 3, 1, 6, 4, 2$ となり、1 から 6 までが 1 回ずつ現れます。7 目盛りの時計を 5 目盛りずつ進むと考えると、図3のように星形を描いてすべての目盛りを通ります。

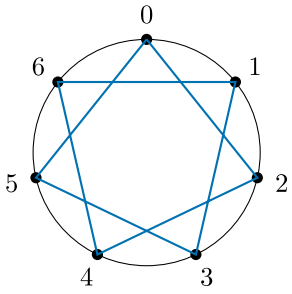


図3　0 から 6 の目盛りを持つ円で、0 から 5 目盛りずつ進むと 0, 5, 3, 1, 6, 4, 2 の順にすべての目盛りを通る

倍数を b で割った余りは重ならない

自然数 a, b は互いに素で、$b \geqq 2$ とする。a, $2a$, …, $(b-1)a$ を b で割った余りは互いに異なり、どれも 0 でない。したがって、余りには $1, 2, \ldots, b-1$ がちょうど 1 回ずつ現れる。

証明

$1 \leqq k \leqq b-1$ とする。ka が b で割り切れたとすると、a と b は互いに素なので k が b で割り切れることになるが、$0 < k < b$ なのでありえない。よって余りに 0 は無い。

次に、ka と la $(1 \leqq k < l \leqq b-1)$ の余りが等しいとすると、差 $(l-k)a$ が b で割り切れる。同じ理由で $l-k$ が b で割り切れることになるが、$1 \leqq l-k \leqq b-2$ なので矛盾する。よって余りは互いに異なる。

1 以上 $b-1$ 以下の値をとる $b-1$ 個の余りが互いに異なるので、1 から $b-1$ までがちょうど 1 回ずつ現れる。 □

この性質を「中国剰余定理」と呼ぶ資料がありますが、それは別の定理です。[1] ここから、整数の重要な性質が二つ導けます。

$ax+by=1$ の整数解

a, b が互いに素な整数ならば、$ax+by=1$ を満たす整数の組 (x, y) が存在する。

証明

まず a, b が自然数の場合を示す。$b = 1$ なら $(x, y) = (0, 1)$ でよい。$b \geqq 2$ なら、上の性質から $a, 2a, \ldots, (b-1)a$ の中に b で割った余りが 1 になるもの xa がある。$xa - 1$ は b の倍数なので、$xa - 1 = -yb$ となる整数 y がとれ、$ax + by = 1$ が成り立つ。

a や b が負のときは、$|a|$, $|b|$ について得た解の x や y の符号を変えればよい。一方が 0 のときは、互いに素であることから他方は ± 1 なので、解はすぐに見つかる。 □

$a = 5$, $b = 7$ なら、余りが 1 になるのは $3 \cdot 5 = 15 = 2 \cdot 7 + 1$ なので、$5 \cdot 3 + 7 \cdot (-2) = 1$ が一つの解です。

フェルマーの小定理

p を素数、a を p で割り切れない整数とすると、

$$a^{p-1} \equiv 1 \pmod{p}$$

証明

a を p で割った余りを考えれば、a は $1 \leqq a \leqq p-1$ としてよい（a を余りに置き換えても a^{p-1} の余りは変わらない）。p は素数で a を割り切らないので、a と p は互いに素である。上の性質から $a, 2a, \ldots, (p-1)a$ を p で割った余りは $1, \ldots, p-1$ を並べかえたものなので、全部かけると

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

左辺は $a^{p-1}(p-1)!$ なので、p は $(p-1)!\,(a^{p-1} - 1)$ を割り切る。素数 p は $1, 2, \ldots, p-1$ のどれも割り切らないから $(p-1)!$ も割り切らず、したがって p は $a^{p-1} - 1$ を割り切る。 □

最後の段で $(p-1)!$ を両辺から消すときに、p が素数であることを使いました。合同式の両辺を同じ数で割ることは一般にはできません（$2 \cdot 3 \equiv 2 \cdot 0 \pmod{6}$ ですが $3 \not\equiv 0 \pmod{6}$）。$p = 7$, $a = 5$ で確かめると、$5^6 = 15625 = 7 \cdot 2232 + 1$ です。

5. 積について閉じた有限集合

集合 G の**どの二つの要素（同じ要素を二度選んでもよい）の積も G の要素になる**とき、G は積について閉じているといいます。1 の n 乗根全体は積について閉じています。$\alpha^n = \beta^n = 1$ なら $(\alpha\beta)^n = \alpha^n \beta^n = 1$ だからです。これに 0 を加えた集合も閉じています。反対に、$\{1, -1, i\}$ は $i \cdot (-1) = -i$ が入っていないので閉じていません。

では、有限個の複素数からなり積について閉じた集合は、ほかにもあるのでしょうか。答えは「これだけ」です。

積について閉じた有限集合

① 0 を含まない n 個の複素数からなり、積について閉じた集合は、1 の n 乗根全体に限る。

② 0 を含む $n+1$ 個の複素数からなり、積について閉じた集合は、1 の n 乗根全体に 0 を加えたものに限る。

①は、2001年の京都府立医科大学の入試で証明させる形で出題されています。

①の証明

集合を $G=\{z_1, z_2, \dots, z_n\}$ とし、G から要素 z を一つ選ぶ。n 個の積 $zz_1, zz_2, \dots, zz_n$ は、閉じていることからどれも G の要素である。また $z\neq 0$ なので、$zz_j=zz_k$ なら $z_j=z_k$ となり、この n 個は互いに異なる。G の要素はちょうど n 個なので、$zz_1, \dots, zz_n$ は $z_1, \dots, z_n$ を並べかえたものにほかならない。

そこで両方の n 個をそれぞれ全部かけると、積の値は等しく

$$z^n z_1 z_2 \cdots z_n = z_1 z_2 \cdots z_n$$

$z_1 z_2 \cdots z_n \neq 0$ で割って $z^n=1$ を得る。z は G のどの要素でもよかったので、G の要素はすべて 1 の n 乗根である。1 の n 乗根はちょうど n 個で、G も n 個の要素からなるので、G は 1 の n 乗根全体に一致する。 □

②は①に帰着できます。G から 0 を除いた n 個の集合を G' とすると、G' の二つの要素の積は G の要素で、しかも 0 でない数どうしの積なので 0 ではありません。よって積は G' の要素であり、G' は 0 を含まない n 個の、積について閉じた集合です。①から G' は 1 の n 乗根全体です。

この種の問題は、知っている発想が無いと手が止まりやすいので、二つの着眼をまとめておきます。

1. 要素 z を全要素にかけても、結果は互いに重ならない（§3・§4 と同じ「重なれば割って矛盾」の議論）。
2. 全要素の積を「かける前」と「かけた後」の二通りに書き、等しいとおいて z^n を取り出す。

①の結論からもう一つ分かることがあります。要素が N 個の、0 を含まず積について閉じた集合は 1 の N 乗根全体なので、各要素は §2 の ξ_m（$n=N$）のどれかで、その位数は $\dfrac{N}{d}$ の形です。つまり

各要素の位数は、要素の個数 N の約数である

ということです。$N=12$ なら §2 の表のとおり、位数は 1, 2, 3, 4, 6, 12 のどれかで、12 の約数でない 5 や 8 は現れません。

1　中国剰余定理は「m, n が互いに素なら、$x \equiv a \pmod{m}$ と $x \equiv b \pmod{n}$ を同時に満たす整数 x が、mn で割った余りとしてただ一つに定まる」という連立合同式の定理です。この節の性質は、その証明に使われる補題にあたります。

塾の授業で配った補足資料をもとに書き直しました。