測度空間の圏

中学 3 年 2 組 7 番 岩根僚太朗

1　はじめに

本日は灘校文化祭および数学研究部にお越しいただき、誠に有難うございます. この記事では主に測度空間の圏に関する事柄を調べます. なお測度論については既知とします. 測度論について知らない方は [2] 等の教科書で勉強されることをおすすめします.

2　圏論におけるいくつかの概念

ここでは圏, 積, 商圏等の概念を定義しますが、厳密な議論は行いません. 詳しくは [1] をご覧下さい.

定義 2.1（圏,hom 集合, 対象の同型）　対象の集合 O と射の集合 A と 2 つの関数

$$A \underset{\mathrm{cod}}{\overset{\mathrm{dom}}{\rightrightarrows}} O$$

からなるものを有向グラフという.

$$A \times_O A := \{\, \langle g, f \rangle \mid g, f \in A \text{ かつ } \mathrm{dom} g = \mathrm{cod} f \}$$

とする. 有向グラフであって、さらに 2 つの関数

$$\begin{array}{ccccccc} O & \xrightarrow{\mathrm{id}} & A & & A \times_O A & \xrightarrow{\circ} & A \\ \cup\!\!\!\!\cup & & \cup\!\!\!\!\cup & & \cup\!\!\!\!\cup & & \cup\!\!\!\!\cup \\ c & \longmapsto & \mathrm{id}_c & & \langle g, f \rangle & \longmapsto & g \circ f \end{array}$$

を持ち、すべての $a \in O$ とすべての $\langle g, f \rangle \in A \times_O A$ について

$$\mathrm{dom}(\mathrm{id}_a) = a = \mathrm{cod}(\mathrm{id}_a)$$

$$\mathrm{dom}(g \circ f) = \mathrm{dom} f, \mathrm{cod}(g \circ f) = \mathrm{cod} g$$

であり、

1.
$$a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{k} d$$
について $k \circ (g \circ f) = (k \circ g) \circ f$.
2. $f : a \to b$,$g : b \to c$ について、$\mathrm{id}_b \circ f = f$ かつ $g \circ \mathrm{id}_b = g$.

を満たすようなものを圏という. b から c へのすべての射の集合を

$$C(b,c) := \{f \mid f \in A, \mathrm{dom} f = b, \mathrm{cod} f = c\}$$

と書き、hom 集合という.a, b が圏 C で同型であるとは、ある射 $e : a \to b$ に対して C の射 $e' : b \to a$ が存在して $e' \circ e = \mathrm{id}_a$かつ $e \circ e' = \mathrm{id}_b$であることをいう.□

すべての集合の“集まり”や任意の 2 つの集合の間の関数の“集まり”のような数学的対象全体の性質を議論するのが圏論の一種の目的としてある訳ですが、Russell の paradox や Burali-Forti の paradox のように、すべての集合の“集まり”やすべての順序数の“集まり”は集合をなさないことが知られています. そこで universe と呼ばれる集合 U を定義し、妥当であると思われる大きさのもの (次に定義する小さな集合) のみを扱います.

定義 2.2（universe, 小さな集合） 次の条件 1 から 5 を満たす集合 U を universe という.

1. $x \in u \in U \Rightarrow x \in U$
2. $u \in U$ かつ $v \in U \Rightarrow \{u, v\}, \langle u, v \rangle, u \times v \in U$(ここで $\langle u, v \rangle$ は順序対、$u \times v$ は直積)
3. $x \in U \Rightarrow Px \in U$ かつ $\bigcup x \in U$(ここで Px は x の冪集合)
4. $\omega \in U$(ここで $\omega := \{0, 1, 2......\}$ はすべての有限順序数の集合)
5. $f : a \to b$ が全射な関数かつ $a \in U$ かつ $b \subset U \Rightarrow b \in U$

$u \in U$ なる集合 u を小さな集合という. 群や位相空間の基底集合が小さな集合であるとき、その群、位相空間は小さな群、小さな位相空間であるという (環や加群等でも同様).□

universe という集合は何となく奇妙な感じがする集合ですが、この詳細を説明するとなるとより集合論的な議論が必要になってくるため、省略させていただきます ([1] の第 I 章第 6 節をご覧下さい).

例 2.3（Set,Grp,Top） ある数学的対象全体を対象の集合とするような圏の例を挙げる.

- 対象をすべての小さな集合、射を任意の 2 つの対象の間の関数すべてであるとすると、これは圏をなす. この圏を **Set** と書く.
- 対象をすべての小さな群、射を任意の 2 つの対象の間の準同型写像すべてであるとすると、これは圏をなす. この圏を **Grp** と書く.
- 対象をすべての小さな位相空間、射を任意の 2 つの対象の間の連続写像すべてであるとすると、これは圏をなす. この圏を **Top** と書く.

定義 2.4（積） 次の条件 1,2 を満たすような対象 $a \times b$ が圏 C に存在するとき、$a \times b$ を a と b の積という.

1. $$a \xleftarrow{p} a \times b \xrightarrow{q} b$$
   なる 2 つの射 p, q が存在する.
2. 下図のような任意の c, f, g について $f = p \circ h$ かつ $g = q \circ h$ であるような射 h が存在し、一意に定ま

る. すなわち下の図式を可換にするような射 h が存在し、一意に定まる.

$$\begin{tikzcd} & c \arrow[dl, "f"'] \arrow[d, "h"] \arrow[dr, "g"] & \\ a & a \times b \arrow[l, "p"'] \arrow[r, "q"] & b \end{tikzcd}$$

このとき $h = \langle f, g \rangle$ と書く.□

例 2.5（**Set**,**Grp**,**Top** における積） **Set**,**Grp**,**Top** で積を考える.

- **Set** における積は直積集合である.
  実際、A, B を集合とすると p, q は $p : A \times B \to A, q : A \times B \to B$ なる *canonical* な射影であり、また $f : C \to A, g : C \to B, x \in C$ として定義 2.4 の図式の $h : C \to A \times B$ を $h(x) = \langle f(x), g(x) \rangle$ なる関数とすると $p \circ h(x) = p(h(x)) = f(x), q \circ h(x) = q(h(x)) = g(x)$ が成り立っている.
- **Grp** における積は群の直積である.
- **Top** における積は位相空間の積である.

定義 2.6（商圏, 同値） C を圏とし、R を C の対象の各対 a, b にhom 集合 $C(a, b)$ 上の同値関係 $R_{a,b}$を割り当てるような関数とする.

$$f, f' \in C(a, b) \text{ が } f R_{a,b} f' \Rightarrow \text{すべての } g : a' \to a \text{ とすべての } h : b \to b' \text{について } (h \circ f \circ g) R_{a',b'} (h \circ f' \circ g)$$

となるとき、R を C 上の合同関係という.B が圏で、対象を C の対象とし、各hom 集合 $B(a, b)$ を $C(a, b)/R_{a,b}$ とするとき、B を合同関係[*1] R による C の商圏といい、C/R と書く. このとき C において対象 a, b が R に関して同値であるとは商圏 C/R において a, b が同型であることをいう. すなわち、ある $f : a \to b, g : b \to a$ が存在して $(g \circ f) R (\mathrm{id}_a)$ かつ $(f \circ g) R (\mathrm{id}_b)$ となるとき a と b は同値であるという.□

例 2.7（**Toph**） 対象をすべての小さな位相空間、射を任意の 2 つの対象の間の連続写像のホモトピー類すべてとすると、これは圏をなし、**Toph** と書くことにする. 定義 2.6 で $C = \mathbf{Top}$ とし、$f R f' \overset{\mathrm{def}}{\Leftrightarrow} f$ が f'とホモトピック、とすると商圏 C/R は **Toph** である. このときの同値は位相空間のホモトピー同値に他ならない.

3 測度空間の圏

$\mathcal{B}_X, \mu_X$をそれぞれ X 上の完全加法族,$\mathcal{B}_X$上の測度とし、可測空間を $X = (X, \mathcal{B}_X)$、測度空間を $X = (X, \mathcal{B}_X, \mu_X)$ というように記号を濫用して表記することがあります. また圏論的な積 (定義 2.4) を単に“積”、直積集合を単に“直積”と記します.

定義 3.1（可測写像, 測度保存写像） X, Y を可測空間として $f : X \to Y$ が可測写像であるとは任意の $E \in \mathcal{B}_Y$に対して $f^{-1}(E) \in \mathcal{B}_X$であることをいう.また X, Y を測度空間として $f : X \to Y$ が測度保存写像であるとは任意の $E \in \mathcal{B}_Y$に対して$\mu_Y(E) = \mu_X(f^{-1}(E))$ であることをいう.□

定義 3.2（可測空間の圏 **Meas**, 測度空間の圏 **MSp**） 対象をすべての小さな可測空間、射を任意の 2 つの対象の間の可測写像すべてであるとするとこれは圏をなし、この圏を **Meas** と書く. 対象をすべての小さな測度

[*1] 任意の R に対して $R \subset R'$となる最小の C 上の合同関係 R'が存在することが証明できる.$(C/R)(a, b)$ を $C(a, b)/R'_{a,b}$と定義することで任意の R に対しても C/R を定義できる.

空間、射を任意の 2 つの対象の間の可測写像でもあり測度保存写像でもあるような写像すべてであるとするとこれは圏をなし、この圏を **MSp** と書く.□

定理 3.3 $\mathcal{E}, \mathcal{F}$ をそれぞれ X, Y の部分集合の有限加法族とすると $K = E \times F(E \in \mathcal{E}, F \in \mathcal{F})$ という形の直積集合 $X \times Y$ の部分集合の有限個の直和として表されるものの全体 $\mathcal{K}$ は有限加法族である.

定義 3.4（直積 σ 代数） 補題 3.3 の $\mathcal{K}$ を含む最小の σ 代数 $\mathcal{B}_{X \times Y} = \mathcal{B}[\mathcal{K}]$ を直積 σ 代数という.□

3.1 積

ここで **Meas** や **MSp** で積を考えてみます.

Meas における積

命題 3.5 **Meas** においてその任意の対象 X, Y に対して積 $X \times Y$ が存在し、それは $(X \times Y, \mathcal{B}_{X \times Y})$ に一致する.

証明 E, F をそれぞれ $\mathcal{B}_X, \mathcal{B}_Y$ の任意の要素とする.定義 2.4 の条件 1 については $p : A \times B \to A, q : A \times B \to B$ が可測写像であることをいえばよいが、p, q を *canonical* な射影とすると $p^{-1}(E), q^{-1}(F) \in \mathcal{B}_{X \times Y}$ であるので成り立つ.条件 2 については M を **Meas** の任意の対象、P を $\mathcal{B}_M$ の任意の要素とし、射 $h : M \to X \times Y$ を $h(P) := \langle f(P), g(P) \rangle$ とすると $h^{-1}(E \times Y) = (p \circ h)^{-1}(E) = f^{-1}(E), h^{-1}(X \times F) = (q \circ h)^{-1}(F) = g^{-1}(F)$ となることと f, g の可測性よりわかる.■

$$\begin{tikzcd}
& M \arrow[dl, "f"'] \arrow[d, "h"] \arrow[dr, "g"] & \\
X & X \times Y \arrow[l, "p"'] \arrow[r, "q"] & Y
\end{tikzcd}$$

MSp における積

命題 3.6 **MSp** において一般に積は存在しない.

証明 測度空間 X, Y の積が存在したとする.**MSp** の射は可測写像でなければならないので命題 3.5 より直積 $X \times Y$ の σ 代数は $\mathcal{B}_{X \times Y}$ であり、射 $p : X \times Y \to X, q : X \times Y \to Y$ は *canonical* な射影である.p, q は測度保存写像であるので $\mu_{X \times Y}$ を積 $X \times Y$ の測度とすると

$$任意の\ E \in \mathcal{B}_X に対して \mu_X(E) = \mu_{X \times Y}(p^{-1}(E))$$

$$任意の\ F \in \mathcal{B}_Y に対して \mu_Y(E) = \mu_{X \times Y}(q^{-1}(F))$$

である. ここで $E = X, F = Y$ とすると上より

$$\mu_X(X) = \mu_{X \times Y}(p^{-1}(X)) = \mu_{X \times Y}(X \times Y) = \mu_{X \times Y}(q^{-1}(Y)) = \mu_Y(Y)$$

となるがこれは一般には成り立たない.■

3.2　測度構造に焦点を当てる

この節では **MSp** での対象の同型性は可測構造に関する条件が強すぎるので **MSp** 上で合同関係を定義し、対象の同値を考えることで測度構造に焦点が当たるようにします.

定義 3.7　測度空間 X, Y と $f, g \in \mathbf{MSp}(X, Y)$ が与えられているとき

$$fR_{X,Y}g \overset{\text{def}}{\Leftrightarrow} f(x) = g(x) \text{ a.e.} x \in X$$

とする.□

ほとんどいたるところで等しいと定義することで可測構造の"大きさ"をあまり気にしなくてよいようにできます.ここで $R_{X,Y}$ は $\mathbf{MSp}(X, Y)$ 上の同値関係であり、R を測度空間の各対 X, Y に $R_{X,Y}$ を割り当てるような関数とするとこれは合同関係です (証明は簡単なので略).これで $\mathbf{MSp}/R$ を考えることができ、そこでは可測構造の同型性に邪魔されません.

4　おわりに

この拙い文章を最後までお読みいただき有難うございました.昨年度に測度論を学んだのですが、可測写像は可測空間の構造を保つような写像であると知ったときに可測空間の圏 (や測度空間の圏) も考えられそうだとふと思ったのがこの内容を考えるきっかけでした.たいした結果は得られたわけではありませんが **MSp** において積は直積集合に直積σ代数や直積測度を付加したものになっているのだろうか、と考えていたので一般に積が存在しないことを知ったときには割と驚きました.そこで **MSp** を弄くって積が存在するような部分圏や商圏が作れないだろうか、と思い考えたのが §3.2 に書いたことなのですが、うまく行かず少し悔しいです.しかしそれなりに面白いことがわかったので個人的には満足しています.来年までに何らかの進捗が得られればまた記事を書くかもしれません.

参考文献

[1] S. マックレーン『圏論の基礎』 三好博之, 高木理訳、丸善出版、2005.
(**原著:** Saunders Mac Lane.*Categories for the Working Mathematician* (Graduate Texts in Mathematics **5**),Springer-Verlag,New York,second edition,1998.)

[2] 伊藤清三『ルベーグ積分入門』(数学選書 4)、裳華房、1963.

Galois 理論

中学 3 年 4 組 10 番　黒木 亮汰

1　はじめに

この記事では体論を抽象的にする方法と, 他の理論との関係を考える.体論でも有名なのは Galois 理論というもので, 一般的に有限次 Galois 理論は分離拡大や正規拡大など拡大体の元の特徴の考察により Galois 拡大というものを定義して, 中間体と Galois 群の部分群の対応 (Galois 対応) を得る.

今回はその Galois 拡大の概念を元の性質を使わずに, 拡大体そのものの性質により定義する.理論の概要から推測して予想を書いたので証明には至っていない。ここでは有限次拡大について考えることにする.

2 章は体論の知識, 3 章は図式の読み方, 4 章は位相, 5 章は空間や可換環の話です.2 章は簡単な説明なので, 既に体論を学んだ方は 3 章から読み進めてください.

2　Galois 理論の概略

[1] から引用. 証明は文献を参照してください.

定義 2.1 (代数閉包)**.** 体 K の代数拡大 L/K で, L の任意の 1 変数多項式の根が L に含まれるものが存在する.それを $\overline{K}$で表す.

定義 2.2 (中間体)**.** 体の拡大 L/K で, L の部分体 M が $M \supset K$ を満たすとき, M を L/K の中間体という.

定義 2.3 (次数)**.** 体の拡大 L/K について, L は K 上のベクトル空間とみなせる.その次元を $[L : K]$ で表し, 拡大次数とする.

定理 2.4. 体の拡大 $L/M, M/K$ について, L/K も体の拡大で, $[L : K] = [L : M][M : K]$

定義 2.5 (最小多項式)**.** 代数拡大 L/K で$\alpha \in L$ とすると, K 上の多項式 $f(x) \neq 0$ で $f(\alpha) = 0$ となるものの中で, 次数が最小となるのは定数倍を除いて一意に定まる.これをαの K 上の最小多項式という.

定義 2.6 (分離拡大)**.** L の任意の元の K 上の最小多項式が$\overline{K}$で重根を持たないとき L を K の分離拡大という.

定理 2.7. 分離拡大 L/K の中間体 M について, L/M は分離

定理 2.8. L/K が分離拡大 $\iff [L : K] = |\mathrm{Hom}_K(L, \overline{K})|$

定義 2.9 (正規拡大)**.** 代数拡大 L/K で, $\alpha \in L$ ならαの K 上の最小多項式が L 上では一次式の積に分解される時, L/K を正規拡大という.

定理 2.10. L/K が正規 $\iff (\phi \in \mathrm{Hom}_K(L, \overline{K}) \Rightarrow \phi(L) \subset L)$

定理 2.11. 正規代数拡大 L/K について, 任意の$\phi \in \mathrm{Hom}(L, L)$ は同型

定義 2.12 (Galois 拡大)**.** 分離かつ正規な拡大 L/K を Galois 拡大という.その時, L の K 自己同型群 $\mathrm{Aut}_K L$ を $\mathrm{Gal}(L/K)$ と書く.

定義 2.13. M が L/K の中間体なら, $H(M) = \{g \in \mathrm{Gal}(L/K) | \forall x \in M, gx = x\}$ とする.

$H \subset \mathrm{Gal}(L/K)$ が部分群なら, $M_H = \{x \in L | \forall g \in H, gx = x\}$ とする.

定義 2.14 (Galois 理論)**.** L/K を有限次 Galois 拡大, $\mathbb{M}$ を中間体の集合, $\mathbb{H}$ を $\mathrm{Gal}(L/K)$ の部分群の集合とする時.
(1)$\mathbb{M} \ni M \mapsto H(M) \in \mathbb{H}, \mathbb{H} \ni H \mapsto M_H \in \mathbb{M}$ は互いの逆写像
(2)M_1, M_2が $\in \mathbb{M}$ が $H_1, H_2 \in \mathbb{H}$ と対応する時,

$$\begin{aligned} M_1 \subset M_2 &\iff H_1 \supset H_2 \\ M_1 \cdot M_2 &\longleftrightarrow H_1 \cap H_2 \\ M_1 \cap M_2 &\longleftrightarrow < H_1, H_2 > \end{aligned}$$

(3)$\sigma \in \mathrm{Gal}(L/K)$ なら

$$\begin{aligned} \sigma(M_1) &\longleftrightarrow \sigma H_1 \sigma^{-1} \\ M/K \text{ が Galois 拡大} &\iff H \lhd \mathrm{Gal}(L/K) \end{aligned}$$

又, $H \lhd \mathrm{Gal}(L/K)$ なら, $\mathrm{Gal}(L/K)$ の元を M に制限することにより, $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/H$

3 形式化

用語の定義は一般的なものと異なることがあります.

定義 3.1 (中間体)**.** 体の拡大 L/K で, L の部分体 M が下図を満たすとき, M を L/K の中間体という.

$$\begin{tikzcd} K \arrow[r, hook] \arrow[dr, hook] & M \arrow[d, hook] \\ & L \end{tikzcd}$$

定義 3.2 (K 自己準同型)**.** $L \supset K$ の自己同型で K を保存するもの (つまり下図が可換となる g) の集合に合成で群構造を入れたものを $\mathrm{Aut}_K L$ と書く.

$$\begin{tikzcd} K \arrow[r, hook] \arrow[dr, hook] & L \arrow[d, "g", "\sim"'] \\ & L \end{tikzcd}$$

体論ではしばしば拡大の次数について調べる. 数値的な発想は体論に限らず, 様々な分野で使われる. 拡大の次数は体上のベクトル空間の基底の数によって定義される. 次数の性質として次の定理がある.
しかし, これでは因数による数の構成が解っても具体的な数値までは解らない. 分離性を仮定すれば次のことが言える.

定義 3.3 (次数)**.** 体の拡大次数 $[L : K]$ を $|\mathrm{Hom}_K(L, \overline{K})|$ と定義する.

定義 3.4 (正規性)**.** $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, L)$ となる時, L/K は正規という.さらに, 分離でもある時, L/K を Galois といい, $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, L) = \mathrm{Gal}(L/K)$

このようにして, 体論を抽象的にできる. ここからは有限次 Galois 理論の仲間について書く.

4 無限次 Galois 理論

主張は有限次の場合とほぼ同じだが,Galois 群に位相を入れる. 中間体と位相が入った Galois 群の閉部分群が対応する.

定義 4.1 (Krull 位相)**.** L に含まれる K の有限次 Galois 拡大 $L \supset M$ によって, $\mathrm{Gal}(L/K)$ の部分群 $\mathrm{Galois}(L/M)$ が構成できる.このような部分群たちを単位元の基本近傍系とする位相が入る.

これで Galois 群は Hausdorff になる

定理 4.2. L/K の中間体の集合 $\mathbb{M}$ に包含で順序を入れる.$\mathrm{Gal}(L/K)$ の閉部分群の集合 $\mathbb{H}$ に包含で順序を入れる.この時,

$$H(\bullet):\mathbb{M}\to\mathbb{H} \qquad M_\bullet:\mathbb{H}\to\mathbb{M}$$

は順序を反転する全単射を導く.

これも正規部分群による剰余群に適当な位相を入れると, 定理 2.4 と類似した性質が成り立つ. Galois 群は有限群の逆極限で書けて, 副有限群とも関係がある.

定理 4.3. K の有限次 Galois 拡大となるような Galois 拡大 L/K の中間体からなる集合 S が次の条件を満たすとする.

- $L=\bigcup\limits_{F\in S}F$
- $F_1,F_2\in S\Rightarrow\exists F_3\in S \quad F_1,F_2\subset F_3$

この時, $\mathrm{Gal}(L/K)\simeq\varprojlim\limits_{F\in S}\mathrm{Gal}(F/K)$

5 体と可換環

ここでは体と可換環のスペクトル理論の関係について書く. 可換環を知らなくても空間と可換環の理論には類似があるので, 空間の言葉で解釈してもらえば大体読める. 拡大をスペクトルの言葉で言うと被覆というものになる. そう考えると中間体の類似は部分被覆ということになる. その前に有限エタール性というのをつかうのでそれを定義する. これは空間で言う所の局所同相写像で, 体の有限次分離拡大の一般化でもある.

定義 5.1. 可換環 R と $\mathrm{Spec}(R)$ に対し, $R_\mathfrak{p}$を R の p による局所化, $\kappa(\mathfrak{p})$ をその剰余体とする.

X,Y をスキームとする.スペクトルと体論が類似しているのは, 次のスペクトルと環の反同値性が関係している.

定理 5.2. $(Ring)\to(Af\text{-}Sch)^o, A\mapsto\mathrm{Spec}A$ は, 環の圏からアフィンスキームの圏への反変関手

定義 5.3. $f:Y\to X$ について, $y\in Y$ として,

- y の開近傍 V で $f|_V\to X$ が局所有限表示となるものがある.
- $x:=f(y)$ とし, 局所環 $\mathcal{O}_{X,x}$の極大イデアルを $\mathfrak{m}_x$と表すとき, $\mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}=\kappa(y)$ で, $\kappa(y)/\kappa(x)$ は有限次分離拡大

を満たす時, f は $y\in Y$ において不分岐という.Y の任意の点で不分岐な時は単に不分岐という.不分岐かつ平坦である被覆をエタール被覆という.

FÉt$/X$ を X 上有限エタールなスキームと X 上の射のなす圏とし, $FSets$ を有限集合と写像のなす圏とする.

定義 5.4. 分離閉体のスペクトラム z からの射 $z\to X$ を X の幾何的点という.

以後, 被覆で有限エタール被覆を指す.X を整閉整域 A のスペクトル $\mathrm{Spec}(A)$ とする.

定義 5.5 (部分被覆)**.** X 上の被覆 $h:Y\to X, h':Y'\to X$ について$\varphi:Y\to Y'$が存在して $h'\circ\varphi=h$ が成り立つ時, h'を h の部分被覆という.このようなφ の集合を $\mathrm{Mor}_X(Y,Y')$ で表す.

$$\begin{tikzcd} Y \arrow[r, "\varphi"] \arrow[dr, "h"'] & Y' \arrow[d, "h'"] \\ & X \end{tikzcd}$$

中間体の場合も埋め込みの合成と埋め込みが可換なので, 定義 3.1 と類似している．中間体は体という対象を見るが, 部分被覆は被覆という射を見る．体論で言う X 準同型はこのφ である．それによって自己準同型群も被覆変換群というものになる．(定義 3.2)

定義 5.6 (被覆変換群)**.** 同型な$\varphi \in \mathrm{Mor}_X(Y,Y)$ の集合に合成で群構造を入れたものを $h: Y \to X$ の被覆変換群と言い, $\mathrm{Aut}_X(Y)$ と書く．

$$\begin{tikzcd} Y \arrow[r, "\varphi"] \arrow[dr, "h"'] & Y \arrow[d, "h"] \\ & X \end{tikzcd}$$

体の場合は $\mathrm{Hom}_K(L,\overline{K})$(定義 3.3) というものを使って次数を定義した.可換環の場合, これはファイバー関手と呼ばれるものを使う．

定義 5.7 (ファイバー関手 (共変))**.** $F_z : F\acute{E}t/X \to FSets, Y \mapsto \mathrm{Mor}_X(z,Y)$

z は分離閉体のスペクトラムで定理 5.2 より Hom の中身を入れ替えて Spec をはずせば $\mathrm{Hom}_K(L,\overline{K})$ と類似が見られる．

定義 5.8 (被覆次数)**.** $|F_z(Y)|$ は,
(1) 任意の点についてある開近傍が存在して, その上での X の既約成分が有限個であるとき
各連結成分上で z によらない.X は連結という仮定から (1) の仮定の下でこれを $h: Y \to X$ の被覆次数と定義する．

ここから (1) を仮定する.定理 2.4 の類似で, m, n 次の射は合成によって mn 次になる．

定理 5.9. $Y \in Ob(F\acute{E}t/X)$、$s \in F_z(Y)$ に対して,

$$f_{Y,s} : \mathrm{Aut}_X(Y) \longrightarrow \mathrm{Mor}_X(z,Y) = F_z(Y)$$

を $g \to g \circ s$ で定めると,
(1)Y が連結なら, 任意の s に対して $f_{Y,s}$は単射
(2)Y が空集合でないなら, (ある s に対して $f_{Y,s}$は全射 $\Longleftrightarrow$ 任意の s に対して $f_{Y,s}$は全射)

定義 5.10 (Galois 性)**.** X 上有限エタールな連結スキーム Y について, 任意の $s \in F$ に対して $f_{Y,s}$が全単射の時,
Y は ($z \to X$ に関して)Galois という．
正規性 (定義 3.4) の $\mathrm{Hom}_K(L,L)(= \mathrm{Aut}_K L)$ と $\mathrm{Hom}_K(L,\overline{K})$ の一致に類似している．
(1) から Galois 性は z に依らないので, $\mathrm{Gal}(Y/X) = \mathrm{Aut}_X(Y)$ と定める.X 上 Galois な対象から成る$F\acute{E}t/X$ の充満部分圏を Gal/X とする．

Galois 理論の類似は副有限化して (逆極限をとって) 得られる．

定理 5.11 (Galois 理論)**.** X 上のある副有限 Galois 被覆 $Z \to X$ の Galois 群 $\mathrm{Gal}(Z/X)$ について, $Z \to X$ の部分被覆と $\mathrm{Gal}(Z/X)$ の閉部分群の間に全単射がある．

この全単射は定理 2.4 の様な性質 (但し副有限化しているので定理 4.2 の様に部分群の開閉を考えなければならない) が成り立つように取れる．エタール基本群というものを使うこともある．これは簡単にいえば絶対ガロア群というものだ．その前に Galois 近傍を定義する．

定義 5.12 (Galois 近傍)**.** $g: X' \to X$ について,

$$\begin{tikzcd} X' \arrow[r, "\alpha"] \arrow[dr, "g"'] & U \arrow[d, "\beta"] \\ & X \end{tikzcd}$$

で, βがエタールであるとき, (α, β) を g のエタール近傍という．
X'を $z, , U \in Ob(\mathrm{Gal}/X), \beta$を構造射として, その同型類がなす集合を考えて, 各同型類から代表を 1 つずつ選んだ集合

を $\mathrm{gal}(z \to X)$ と表す.

$$\begin{tikzcd} z \arrow[r] \arrow[dr] & Y \arrow[d, "(\text{構造射})"] \\ & X \end{tikzcd}$$

$Y, Y' \in \mathrm{gal}(z \to X)$ に対して

$$\begin{tikzcd} z \arrow[r] \arrow[dr] & Y' \arrow[d, dotted, "f"'] \arrow[dr] & \\ & Y \arrow[r] & X \end{tikzcd}$$

を可換にする f が存在する (存在すれば一意) ときに $Y \leqslant Y'$とすると, $(\mathrm{gal}(z \to X))$ は有向集合となる.

エタール基本群を定義するときは極限をとるので, その前に推移写像を入れる. 具体的には, $f : Y' \to Y$ を Gal/X に属する射とした時に、$s \in F_z(Y')$ に対して,

$$\begin{tikzcd} \mathrm{Aut}_X(Y') \arrow[r, "f_{Y',s}", "\sim"'] \arrow[d, "\psi_{f,s}"'] & F_z(Y') \arrow[d, "F_z(f)"] \\ \mathrm{Aut}_X(Y) \arrow[r, "f_{Y,F_z(f)(s)}", "\sim"'] & F_z(Y) \end{tikzcd}$$

を可換にする$\psi_{f,s}$を推移写像とする.これは s によらない.$g \in \mathrm{Aut}_X(Y')$ をとると, 下図が可換になる.

$$\begin{tikzcd} Y' \arrow[r, "g"] \arrow[d, "f"'] & Y' \arrow[d, "f"] \\ Y \arrow[r, "\psi_{f,s}(g)"] & Y \end{tikzcd}$$

定義 5.13 (エタール基本群)**.** $z \to X$ を基点とするエタール基本群を$\pi(X, z) := \varprojlim_{Y \in \mathrm{gal}(z \to X)} \mathrm{Aut}_X(Y)$ とする.これは $\mathrm{gal}(x \to X)$ に依らない.これは副有限群になる.

定理 4.3 の右辺と似ているのでその類似からか, 定理 5.11 と似た (連結副有限エタール被覆とエタール基本群の) 対応が成り立つ.

グロタンティークの Galois 理論というものがあって, それの出発点となる次の定理がある.

定理 5.14. $\pi(X, z)$ による連続な左作用を持つ有限集合と, $\pi(X, z)$ 同変関手を持つ圏を$\pi(X, z)$-$FSets$ と表す.
この時, F_zは$F\acute{E}t/X$ から$\pi(X, z)$-$FSets$への圏同値を引き起こす.

6　おわりに

読んでいただきありがとうございました. Galois 理論を抽象化する試みは既になされているのですが, 文献 [2] はまだ読んでいないので, 体論と可換環論の類似について具体例をまとめておきたく, 文献 [4],[5] を参考に考察しました.

参考文献

[1] 雪江明彦：代数学 2,3　日本評論社.
[2] Grothendieck, A., Raynaud, M.: *Revêtements étales et groupe fondamental*
[3] 川又雄二郎：代数多様体論
[4] 森下昌紀：結び目と素数
[5] 斎藤秀司 , 佐藤周友：代数的サイクルとエタールコホモロジー

ディィリクレのＬ関数の特殊値について

高校１年２組３８番　知念慶

1　はじめに

本日は灘校文化祭および数学研究部にお越しいただき、誠にありがとうございます。この記事では、去年の部誌で書いたディリクレのＬ関数の特殊値について、扱ってなかったものや、別の級数の値を求めていきたいと思います。単調で、計算ばかりのつまらない内容になりますが、読んでいただけると嬉しいです。予備知識としては高校数学程度を仮定し、それ以外は書いていきたいと思います。

2　予備知識

2.1　項別微分

以下で一様収束などの定義を述べていく。

定義 1.1（一様収束）

Ｉを定義域とする関数列 $\{f_n(x)\}_{n=1,2,...}$ がＩを定義域とする関数 f に一様収束するとは、任意の正実数 ϵ に対してある自然数Nがあって、$n > N$ を満たす任意の自然数 n とＩに属する任意の x に対して

$$|f_n(x) - f(x)| < \epsilon$$

が成り立つことをいう

定義 1.2（広義一様収束）

Ｉを定義域とする関数列 $\{f_n(x)\}_{n=1,2,...}$ が広義一様収束しているとはＩに含まれる任意の有界閉区間をとったとき、関数列 $\{f_n(x)\}_{n=1,2,...}$ の定義域をそこに制限すると一様収束していることをいう。

定理 1.3（項別微分）

１回微分可能な関数の列 $\{f_n(x)\}_{n=1,2,...}$ がある関数 f に一様収束しており、導関数の列 $\{f_n^{`}(x)\}_{n=1,2,...}$ がある関数 $g$ に広義一様収束しているのなら $f$ も一回微分可能で $f^{`} = g$ が成り立つ。

無限級数の一様収束の判定法には次のようなものがある。

定理 1.4（ワイエルシュトラスのMテスト）

関数列 $\{f_n(x)\}_{n=1,2,...}$ に対して数列 M_n で次の条件

- 定義域内の任意の x に対して $|f_n(x)| < M_n$ が成り立つ。
- $\sum_{n=1}^{\infty} M_n$ が収束する。

を満たすものが存在するとき、$\sum_{m=1}^{n} f_m(x)$ は一様収束する。

このワイエルシュトラスのMテストを用いると次のことがわかる。

定理 1.5

$m > 1$ に対して

$$\sum_{k=1}^{n} \frac{\sin 2kx}{k^m}$$

は一様収束する。分子が $\cos 2kx$ のときも同様。

詳しく知りたい方は参考文献の URL を参照してください。

2.2 微分方程式

微分方程式の解の公式

未知の関数 $f(x)$ があって、この関数が定数 a と関数 $Q(x)$ に対して、

$$\frac{d}{dx}f(x) = af(x) + Q(x)$$

を満たすとき、$f(x)$ は

$$f(x) = e^{ax}\left(C + \int_0^x Q(t)e^{-at}dt\right)$$

となる (ここで C は積分定数)

証明

まず移項すると

$$\frac{d}{dx}f(x) - af(x) = Q(x)$$

これに e^{-ax} をかけて

$$e^{-ax}\frac{d}{dx}f(x) + (-ae^{-ax}f(x)) = e^{-ax}Q(x)$$
$$e^{-ax}\frac{d}{dx}f(x) + (\frac{d}{dx}e^{-ax})f(x) = e^{-ax}Q(x)$$

ここで積の微分公式を逆に使うと、

$$\frac{d}{dx}(e^{-ax}f(x)) = e^{-ax}Q(x)$$

これを積分して

$$e^{-ax}f(x) = C + \int_0^x Q(t)e^{-at}dt$$
$$\therefore f(x) = e^{ax}\left(C + \int_0^x Q(t)e^{-at}dt\right)$$

よって示された。これは 2 変数関数についても、1 つの文字に関する微分方程式であれば、もう一方の変数を定数として考えれば使用できる。

3　L 関数の特殊値の求め方

さてどうやってL関数の特殊値を求めるかですが、まずL関数を定義します。

定義 2.1

以下の条件を満たす写像 $\chi:\mathbb{Z}\to\mathbb{C}$ を指標nのディリクレ指標という

- $\chi(a+n)=\chi(a)$ m
- a と n が互いに素でないことと $\chi(a)=0$ は同値である
- a と b が互いに素であるならば、$\chi(a)\chi(b)=\chi(ab)$

定義 2.2

指標nのディリクレ指標に対し、ディリクレのL関数を以下のように定義する。

$$L(s)=\sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}$$

それでは、ある結論を導くための補題を示していきたいと思います。

定義.23

指標nのディリクレ指標 $\chi(a)$ に対し、ガウス和 $\tau(\chi)$ を以下のように定義する。

$$\tau(\chi)=\sum_{a=1}^{n-1}\chi(a)e^{\frac{2i\pi a}{n}}$$

定理 2.4

$$\sum_{a=1}^{n-1}\chi(a)e^{\frac{2i\pi am}{n}}=\overline{\chi(m)}\tau(\chi)$$

これを証明するために次の補題を示す。

補題 2.5

集合Aを $A=\left\{a_m \mid 1\leqq a_m\leqq n,\ 1\leqq m\leqq\phi(n), a_{\mathrm{m}}\text{ とnは互いに素}\right\}$ とする。Aからとりだしたある一つの元をbとすると、$bA=\left\{ba \mid a\in A\right\}=A$

証明

まず、ba_m は a_m とnが互いに素なので、nと互いに素である。また、

$$ba_i\equiv ba_j \mod n \quad (i\neq j)$$

とするとbとmは互いに素なので $a_i\equiv a_j \mod n$ となり矛盾する。よってb A の元はすべて異なり、b A と A の元の個数はどちらも $\phi(n)$ になる。よって示された。

補題 1.6

a と m が互いに素のとき、$a^{\phi(n)} \equiv 1 mod n$

証明

補題 1.5 において b=a とすると aA=A より、

$$aa_1 \cdot aa_2 \cdot \ldots \equiv a_1 a_2 \ldots a_{\phi(n)} \mod n$$
$$a^{\phi(n)} \cdot (a_1 a_2 \ldots a_{\phi(n)} \equiv a_1 a_2 \ldots a_{\phi(n)} \mod n$$

$a_1, a_2, \ldots a_{\phi(n)}$ はすべてｎと互いに素なので $a^{\phi(n)} \equiv 1 \mod n$ となる

定理 2.4 の証明

補題 1.6 より $\chi(a^{\phi(n)}) = \chi(1) = 1$ なので $\chi(a)$ は１の累乗根である。よって

$$\overline{\chi(a)} = \frac{1}{\chi(a)}$$

となり、定理 1.4 は次のようになる。

$$\sum_{a=1}^{n-1} \chi(am) e^{\frac{2i\pi am}{n}} = \sum_{a=1}^{n-1} \chi(am \mod n) e^{\frac{2i\pi(am \mod n)}{n}} = \tau(\chi)$$

ｍとｎが互いに素のとき、$am \mod n$ は１からｎ - １のすべての数字を回るのでこの式は正しい。次にと n が互いに素でないとき、最大公約数をｄ、ｎをｄで割ったものをｇとすると、

$$\begin{aligned}\sum_{a=1}^{n-1} \chi(a) e^{\frac{2i\pi am}{n}} &= \sum_{a=1}^{n-1} \chi(a) e^{\frac{2i\pi am}{dg}} \\ &= \sum_{k=1}^{n} \sum_{\frac{am}{d} \mod g=k} \chi(a) e^{\frac{2i\pi k}{g}}\end{aligned}$$

ここで $\frac{am}{d} \mod g = k$ の解を $a_1, a_2, \ldots a_t$ は $\frac{am}{d} \mod g = 1$ の解 $b_1, b_2, \ldots b_t$ のｋ倍になるのである定数ｃを用いて

$$\begin{aligned}\sum_{a=1}^{n-1} \chi(a) e^{\frac{2i\pi am}{n}} &= c \sum_{\frac{am}{d} \mod g=1} \chi(a) \\ &= 0 \\ &= \overline{\chi(m)} \tau(\chi)\end{aligned}$$

よって示された。

さて、Ｌ関数をもとめる方法を示す。

定理 1.7

関数列 $\{f_n(x)\}_{n=1,2,\ldots}, \{g_n(x)\}_{n=1,2,\ldots}$ を以下のように定める。

$$f_{2n+1}(x) = (-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\sin(2mx)}{m^{2n+1}} \qquad f_{2n}(x) = 2\cdot(-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\cos(2mx)}{m^{2n}}$$

$$g_{2n+1}(x) = (-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\cos(2mx)}{m^{2n+1}} \qquad g_{2n}(x) = 2\cdot(-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\sin(2mx)}{m^{2n}}$$

このとき、L関数の特殊値は以下のように定まる

1. $\chi(-1) = 1$ のとき

$$L(2r,\chi) = \overline{\tau^{-1}(\chi)} \sum_{k=1}^{n-1} \overline{\chi(k)} 2^{2r-1}(-1)^r f_{2r}(\frac{k\pi}{n}) \qquad L(2r+1,\chi) = \overline{\tau^{-1}(\chi)} \sum_{k=1}^{n-1} \overline{\chi(k)}(-4)^r g_{2r+1}(\frac{k\pi}{n})$$

2. $\chi(-1) = -1$ のとき

$$L(2r,\chi) = \overline{\tau^{-1}(\chi)} \sum_{k=1}^{n-1} \overline{\chi(k)} 2^{2r-1}(-1)^r g_{2r}(\frac{k\pi}{n}) \qquad L(2r+1,\chi) = \overline{\tau^{-1}(\chi)} \sum_{k=1}^{n-1} \overline{\chi(k)}(-4)^r f_{2r+1}(\frac{k\pi}{n})$$

証明

1 だけ証明する。2 は 1 と同様にできる。

$$\sum_{k=1}^{n-1} \chi(k) \sum_{m=1}^{\infty} \frac{e^{\frac{2imk\pi}{n}}}{m^{2r}} = \sum_{m=1}^{\infty} \frac{\sum_{k=1}^{n-1} \chi(k) e^{\frac{2imk\pi}{n}}}{m^{2r}}$$

定理 1.4 より

$$\begin{aligned}\sum_{k=1}^{n-1} \sum_{m=1}^{\infty} \frac{e^{\frac{2i\pi km}{n}}}{m^{2r}} &= \tau(\chi) \sum_{m=1}^{\infty} \frac{\overline{\chi(m)}}{m^{2r}} \\ &= \tau(\chi)\overline{L(2r,\chi)}\end{aligned}$$

また、

$$\begin{aligned}\sum_{k=1}^{n-1} \sum_{m=1}^{\infty} \frac{e^{\frac{2i\pi km}{n}}}{m^{2r}} &= \sum_{m=1}^{\infty} \frac{\sum_{k=1}^{n-1} \chi(k) e^{\frac{2imk\pi}{n}}}{m^{2r}} \\ &= \sum_{k=1}^{n-1} \chi(k) \sum_{m=1}^{\infty} \frac{\cos(\frac{2mk\pi}{n})}{m^{2r}} + \sum_{m=1}^{\infty} \frac{\sum_{k=1}^{n-1} \chi(k) \sin(\frac{2mk\pi}{n})}{m^{2r}}\end{aligned}$$

ここで

$$\begin{aligned}2\cdot\sum_{k=1}^{n-1} \chi(k) \sin(\frac{2mk\pi}{n}) &= \sum_{k=1}^{n-1} \chi(k) \sin(\frac{2mk\pi}{n}) + \sum_{k=1}^{n-1} \chi(n-k) \sin(\frac{2m(n-k)\pi}{n}) \\ &= \sum_{k=1}^{n-1} \chi(k) \sin(\frac{2mk\pi}{n}) + \sin(\frac{2m(n-k)\pi}{n}) \\ &= 0\end{aligned}$$

よって sin の部分は消えて

$$\begin{aligned}\sum_{k=1}^{n-1} \sum_{m=1}^{\infty} \frac{e^{\frac{2i\pi km}{n}}}{m^{2r}} &= \sum_{k=1}^{n-1} \sum_{m=1}^{\infty} \frac{\cos(\frac{2mk\pi}{n})}{m^{2r}} \\ &= \sum_{k=1}^{n-1} \chi(k) 2^{2r-1}(-1)^r f_{2r}(\frac{k\pi}{n})\end{aligned}$$

以上より

$$L(2r,\chi)=\overline{\tau^{-1}(\chi)}\sum_{k=1}^{n-1}\overline{\chi(k)}2^{2r-1}(-1)^r f_{2r}(\frac{k\pi}{n})$$

よって示された。$L(2r+1,\chi)$ の場合も同様の計算で示せる。■

定理 1.7 から関数列 $\{f_n(x)\}_{n=1,2,\dots},\{g_n(x)\}_{n=1,2,\dots}$ を有限和で表わせればよいことがわかる。次の章ではそれをやっていく。

4 三角関数の無限和

4.1 $f_n(x)$

関数列 $\{f_n(x)\}_{n=1,2,\dots}$ を求めるために以下のような形式的べき級数を定める。

$$F(x,y)=\sum_{n=1}^{\infty}f_{n+1}(x)y^{n-1}$$

この形式的べき級数を閉じた形で求めたい。関数列 $\{f_n(x)\}_{n=1,2,\dots}$ については以下のことが分かってる。

$$\frac{d}{dx}f_n(x)=f_{n-1}(x)$$

２章で $f_n(x)$ が項別微分できることが分かるので、微分すると導かれる。このことから形式的べき級数 $F(x,y)$ は以下の偏微分方程式を満たす。

$$\frac{d}{dx}F(x,y)=\frac{d}{dx}f_2(x)+yF(x,y)$$

この偏微分方程式はｘでしか微分してないので、ｙを定数とみれば実質ｘの微分方程式である。これを２章の微分方程式の解の公式を用いると、

$$F(x,y)=c_1(y)e^{xy}+e^{xy}\int_0^x f_1(t)e^{-ty}dt$$

ここで $c_1(y)$ はｙの任意の関数である。ここで $f_1(x)$ を求める必要があるので次の定理を証明する

定理 3.1.1

$$\sum_{m=1}^{\infty}\frac{\sin(mx)}{m}=\frac{\pi-x}{2}$$

証明

以下の関数を考える。

$$h_m(x)=\sum_{k=1}^{m}\frac{\sin(2kx)}{k}$$

この関数の極限をとれば $f_1(x)$ になる。微分すると

$$\frac{d}{dx}h_m(x)=2\sum_{k=1}^{m}\cos(2kx)$$

この和を求めるために以下の補題を示す。

補題 3.1.2

$$\sum_{k=0}^{m}\sin(2kx)=\frac{\sin((m+1)x)\sin(mx)}{\sin x}\quad \sum_{k=0}^{m}\cos(2kx)=\frac{\sin((m+1)x)\cos(mx)}{\sin x}$$

証明

$$\begin{aligned}\sum_{k=0}^{m}e^{2ikx}&=\frac{1-e^{2i(m+1)x}}{1-e^{2ix}}\\&=\frac{1-e^{2i(m+1)x}}{e^{ix}(e^{-ix}-e^{ix})}\\&=\frac{e^{i(m+1)x}(e^{-i(m+1)x}-e^{i(m+1)x})}{e^{ix}(e^{-ix}-e^{ix})}\\&=\frac{e^{imx}\sin((m+1)x)}{\sin x}\end{aligned}$$

この関数の実部と虚部を考えると与式が得られる ■

よって

$$\frac{d}{dx}h_m(x)=\frac{2\sin((m+1)x)\cos(mx)-2\sin x}{\sin x}$$

これを積分すると、

$$\begin{aligned}h_m(x)&=\int_1^x\frac{2\sin((m+1)t)\cos(mt)-2\sin t}{\sin t}dt+C\\&=\int_1^x\frac{\sin((2m+1)t)+\sin t-2\sin t}{\sin t}dt+C\\&=-x+1+\int_1^x\frac{\sin((2m+1)t)}{\sin t}dt+C\end{aligned}$$

ここで

$$\begin{aligned}\int_1^x\frac{\sin((2m+1)t)}{\sin t}dt&=-\int_1^x\frac{1}{\sin t}(\frac{\cos((2m+1)t)}{2m+1})'dt\\&=-\left[\frac{\cos((2m+1)t)}{(2m+1)\sin t}\right]_1^x+\frac{1}{2m+1}\int_1^x\frac{\cos((2m+1)t)\cos t}{\sin^2 t}dt\\&=-\left[\frac{\cos((2m+1)t)}{(2m+1)\sin t}\right]_1^x+\frac{1}{2m+1}(H(x)-H(1))\end{aligned}$$

これの極限をとると、$H(x)$ が発散せず、$\sin t$ が 0 にならなければ 0 になる。よって $x\neq 0,\pi$ のとき

$$\lim_{m\to\infty}h_m(x)=-x+1+C$$

となる。積分定数の値を確定させるために $x=\frac{\pi}{2}$ を代入すると

$$\begin{aligned}0&=-\frac{\pi}{2}+1+C\\ \therefore C&=\frac{\pi}{2}-1\end{aligned}$$

よって示された。この証明により、定理 1.5 の $m=1$ の場合については広義一様収束することがわかる。■

よって

$$F(x,y)=(c_1(y)+\frac{\pi}{2}+\frac{1}{y^2})e^{xy}-\frac{\pi}{2y}+\frac{x}{y}+\frac{1}{y^2}$$

ここで以下の補題を示す。

補題 3.1.3

$$\lim_{x\to\pi} f_1(x) - \lim_{x\to 0} f_1(x) = -\pi \quad \lim_{x\to\pi} f_n(x) = \lim_{x\to 0} f_n(x)$$

証明

まず初めに 2 番目の式から示す。$f_n(\frac{\pi}{2}+t) - f_n(\frac{\pi}{2}-t)$ を考える $(0 < t < \pi)$

$$\begin{aligned} f_{2n}(\frac{\pi}{2}+t) - f_{2n}(\frac{\pi}{2}-t) &= 2\cdot(-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\cos(m(\pi+2t)) - \cos(m(\pi-2t))}{m^{2n}} \\ &= -2\cdot(-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{2\sin(m\pi)\sin 2t}{m^{2n}} \\ &= 0 \end{aligned}$$

よって

$$\lim_{t\to\frac{\pi}{2}} f_{2n}(\frac{\pi}{2}+t) - f_{2n}(\frac{\pi}{2}-t) = 0$$

奇数の場合も同様に

$$\begin{aligned} f_{2n+1}(\frac{\pi}{2}+t) - f_{2n+1}(\frac{\pi}{2}-t) &= (-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{\sin(m(\pi+2t)) - \sin(m(\pi-2t))}{m^{2n+1}} \\ &= (-\frac{1}{4})^n \sum_{m=1}^{\infty} \frac{2\sin 2mt\cos(m\pi)}{m^{2n+1}} \end{aligned}$$

これの極限をとって

$$\begin{aligned} \lim_{t\to\frac{\pi}{2}} f_{2n+1}(\frac{\pi}{2}+t) - f_{2n+1}(\frac{\pi}{2}-t) &= (-\frac{1}{4})^n \sum_{m=1}^{\infty} \lim_{t\to\frac{\pi}{2}} \frac{2\sin 2mt\cos(m\pi)}{m^{2n+1}} \\ &= 0 \end{aligned}$$

よって示された。なお、級数の項の入れ替えや、極限と総和の交換などをしたが、絶対収束して、一様収束もするので問題ない。■

よって $F(\pi,y) - F(0,y) = 0$ なので

$$\begin{aligned} (c_1(y)+\frac{\pi}{2}+\frac{1}{y^2})e^{\pi y} - \frac{\pi}{2y} + \frac{\pi}{y} + \frac{1}{y^2} - (c_1(y)+\frac{\pi}{2}+\frac{1}{y^2} - \frac{\pi}{2y} + \frac{1}{y^2}) = 0 \\ (e^{\pi y}-1)(c_1(y)+\frac{\pi}{2}+\frac{1}{y^2}) + \frac{\pi}{y} = 0 \end{aligned}$$

$$\therefore c_1(y) + \frac{\pi}{2} + \frac{1}{y^2} = -\frac{\pi}{y(e^{\pi y}-1)}$$

以上より

$$F(x,y) = -\frac{\pi}{y(e^{\pi y}-1)}e^{xy} - \frac{\pi}{2y} + \frac{x}{y} + \frac{1}{y^2}$$

あとはこの関数のべき級数展開を考えればいい。B_n をベルヌーイ数とすると

$$y^2F(x,y) = -\left(\sum_{k=0}^{\infty}\frac{B_k}{k!}(\pi y)^k\right)\left(\sum_{m=0}^{\infty}\frac{(xy)^n}{n!}\right) - \frac{\pi y}{2} + xy + 1$$

y^n の係数を考えると、

$$\begin{aligned} f_n(x) &= -\sum_{k+m=n}\frac{B_k}{k!}\pi^k\frac{x^m}{m!} \\ &= -\sum_{k=0}^{n}\frac{\pi^k}{k!(n-k)!}B_kx^{n-k} \end{aligned}$$

これで関数列 $\{f_n(x)\}_{n=1,2,...}$ が求まった。

4.2 $g_n(x)$

$g_n(x)$ に対しても同じようにして求めることができる。関数列 $\{g_n(x)\}_{n=1,2,...}$ に対して以下のような形式的べき級数を考える。

$$G(x,y) = \sum_{n=1}^{\infty} g_{n+1}(x)y^{n-1}$$

この形式的べき級数を閉じた形で求めよう。$g_n(x)$ については以下のことがわかってる。

$$\frac{d}{dx}g_n(x) = g_{n-1}(x) \quad \lim_{x\to\pi} g_n(x) = \lim_{x\to 0} g_n(0)$$

１番目も２番目も 4.1 と同じようにしてわかる。よって $G(x,y)$ は以下の偏微分方程式を満たす。

$$\frac{d}{dx}G(x,y) = \frac{d}{dx}g_2(x) + yG(x,y)$$

これを解いて

$$G(x,y) = c_2(y)e^{xy} + e^{xy}\int \mathrm{g}_1(x)e^{-ty}dx$$

ここで $c_2(y)$ はｙの任意の関数である。これを求めるには $g_1(x)$ を求める必要があるので、以下の定理を示す。

定理 3.2.1

$$\sum_{m=1}^{\infty}\frac{\cos 2mx}{m} = -(\log 2 + \log(\sin x))$$

証明

以下の関数を考える。

$$h_m(x) = \sum_{k=1}^{m}\frac{\cos 2mx}{m}$$

この関数はmの極限をとれば $g_1(x)$ となる。微分すると

$$\frac{d}{dx}h_m(x) = -2\sum_{k=1}^{m}\sin 2mx$$

定理 3.1.2 より

$$\frac{d}{dx}h_m(x) = -\frac{2\sin((m+1)x)\sin(mx)}{\sin x}$$

これを積分すると

$$\begin{aligned} h_m(x) &= -\int_1^x \frac{2\sin((m+1)t)\sin(mt)}{\sin t}dt + C \\ &= \int_1^x \frac{\cos((2m+1)t) - \cos t}{\sin t}dt + C \\ &= -\log(\sin x) + \log(\sin 1) + \int_1^x \frac{\cos((2m+1)t)}{\sin t}dt + C \end{aligned}$$

ここで

$$\begin{aligned} \int_1^x \frac{\cos((2m+1)t)}{\sin t}dt &= \int_1^x \frac{1}{\sin t}\left(\frac{1}{2m+1}\sin((2m+1)t)\right)^{`} dt \\ &= [\frac{\sin((2m+1)t)}{(2m+1)\sin t}]_1^x + \frac{1}{2m+1}\int_1^x \frac{\sin((2m+1)t)\cos t}{\sin^2 t}dt \\ &= [\frac{\sin((2m+1)t)}{(2m+1)\sin t}]_1^x + \frac{1}{2m+1}(H(x) - H(1)) \end{aligned}$$

mの極限をとると、$H(x)$ が発散せず、$\sin t$ が 0 にならなければよいので、$x \neq \pi, 0$ で

$$\lim_{m\to\infty} = -\log(\sin x) + \log(\sin 1) + C$$

となる。ここで積分定数の値を求めるために $x = \frac{\pi}{2}$ を代入すると

$$\begin{aligned} \sum_{m=1}^{\infty}\frac{(-1)^m}{m} &= \log(\sin 1) + C \\ \therefore C &= -\log 2 - \log(\sin 1) \end{aligned}$$

よって示された。■

これを偏微分方程式の解に代入すると

$$G(x,y) = c_2(y)e^{xy} + e^{xy}\int_0^x \log(2\sin t)\ e^{-ty}dt$$

ここで以下の補題を示す。

補題 3.2.2

$$\lim_{x\to\pi} g_n(x) = \lim_{x\to 0} g_n(x)$$

証明

補題 3.1.3 と同様にして示せる。■

よって $G(\pi,y) - G(0,y) = 0$ で、

$$e^{\pi y}\left(c_2(y) - \int_0^\pi \log(2\sin t)\ e^{-ty}dt\right) - c_2(y) = 0$$

$$\therefore c_2(y) = -\left(1 + \frac{1}{e^{\pi y} - 1}\right) \int_0^\pi \log(2\sin t)\ e^{-ty} dt$$

ここで、数列 A_n を以下のように定義する。

$$A_n = \int_0^\pi t^n \log(2\sin t) dt$$

すると $c_2(y)$ は以下のように書ける。

$$c_2(y) = -\left(1 + \frac{1}{e^{\pi y} - 1}\right) \sum_{n=0}^{\infty} (-1)^n \frac{A_n}{n!} y^n$$

よって

$$yG(x,y) = -y\ e^{xy} \left(1 + \frac{1}{e^{\pi y} - 1}\right) \sum_{n=0}^{\infty} (-1)^n \frac{A_n}{n!} y^n + ye^{xy} \int_0^x \log(2\sin t) e^{-ty} dt$$

これをべき級数展開すれば $g_n(x)$ がえられるが、これは積分や無限和を用いなければ表わすことができない。

5　終わりに

ここまで読んでいただきありがとうございました。この文章の内容については、僕の知識が足りないために厳密性のかけているところもあったかと思われます。また、TEX を使い慣れていないために、読みにくい箇所がいくつかあります。ごめんなさい。これらについてはこれからも精進して改善していきたいと思います。今回の部誌の内容についてですが、去年考えたことを別の方法で考え直して、そうすることによって去年もとめられなかった $g_n(x)$ についても考えることができました。ただ $g_n(x)$ の表示についてはまだ改善の余地があるとおもうので、引き続き研究していきたいと思います。

それでは引き続き灘校文化祭をお楽しみください。

6　参考文献

https://lecture.ecc.u-tokyo.ac.jp/～nkiyono/2010/hira10-12.pdf（項別積分）
http://hooktail.sub.jp/mathlnPhys/constOneLinearDiffEq/(微分方程式)
～は半角で打ち込んでください。

ロピタルの定理の証明

高校 1 年 4 組 15 番　黒田直樹

1　はじめに

本日は数学研究部にお越しいただきありがとうございます. この記事では, この記事では, 極限に関する有名な定理, ロピタルの定理を証明したいと思います. 基礎知識は特に必要ありませんが, 微分積分の知識があると分かりやすいと思います.

2　準備

ここで使う用語の定義や定理の証明などをしていきます.$a := b$ で a を b(に等しいもの) として定義する,$\forall$ で任意の,$\exists$ で条件を満たすものが存在する, という意味です.

定義 2.1

$$[a, b] := \{x : a \leqq x \leqq b\}, (a, b) := \{x : a < x < b\}$$

定義 2.2

$$\lim_{x\to a} f(x) = b \underset{def}{\iff} \forall\epsilon > 0, \exists\delta > 0, 0 < |x - a| < \delta \Rightarrow |f(x) - b| < \epsilon$$

難しいことを言っているようですが, 結局 x が a に十分近い時,$f(x)$ は b に十分近くなるということです. ここで $x \neq a$ の時について考えてることに注意してください ($\because 0 < |x - a|$)

例　$f(x) = 0(x = 0)\quad 1(x \neq 0)$ という関数について考えたとき,$\lim_{x\to 0} f(x) = 1$

命題 2.3

$$1\ \lim_{x\to a}(f(x) + g(x)) = \lim_{x\to a} f(x) + \lim_{x\to a} g(x)$$

$$2\ \lim_{x\to a}(f(x)g(x)) = \lim_{x\to a} f(x) \lim_{x\to a} g(x)$$

証明　$\lim_{x\to a} f(x) = m, \lim_{x\to a} g(x) = n$ とする.

$$1\ \forall\epsilon > 0, \exists\delta_1 > 0, 0 < |x - a| < \delta_1 \Rightarrow |f(x) - m| < \frac{\epsilon}{2}$$

$$\forall\epsilon > 0, \exists\delta_2 > 0, 0 < |x - a| < \delta_2 \Rightarrow |g(x) - n| < \frac{\epsilon}{2}$$

ここで,$\delta_0 = \max(\delta_1, \delta_2)$ とおくと,

$$\forall\epsilon > 0, \exists\delta_0 > 0, 0 < |x - a| < \delta_0 \Rightarrow |f(x) + g(x) - (m + n)| \leqq |f(x) - m| + |g(x) - n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon ■$$

2 まず,ϵ は小さければより良いので,$\epsilon < 1$ としてよい.

$$\forall\epsilon > 0, \exists\delta_1 > 0, 0 < |x-a| < \delta_1 \Rightarrow |f(x) - m| < \frac{\epsilon}{|m|+|n|+1}(<1)$$

$$\forall\epsilon > 0, \exists\delta_2 > 0, 0 < |x-a| < \delta_2 \Rightarrow |g(x) - n| < \frac{\epsilon}{|m|+|n|+1}(<1)$$

ここで,$\delta_0 = \max(\delta_1, \delta_2)$ とおくと,

$$0 < \forall\epsilon < 1, \exists\delta_0 > 0, 0 < |x-a| < \delta_0 \Rightarrow |f(x)g(x) - mn| \leqq |g(x)(f(x)-m)| + |m(g(x)-n)|$$

$$\leqq (|g(x)-n| + |n|)|f(x)-m| + |m||(g(x)-n)| < (1+|n|)\frac{\epsilon}{|m|+|n|+1} + \frac{\epsilon|m|}{|m|+|n|+1} = \epsilon\blacksquare$$

定義 2.4

$\lim_{x\to a} f(x) = f(a)$ の時, $f(x)$ は $x = a$ で連続という.$[a, b]$ の各点で $f(x)$ が連続の時, $f(x)$ は $[a, b]$ で連続という.

私達の知ってる関数のほとんどは連続ですが, 例えば $f(x) = \frac{1}{x}$ などは $x = 0$ で連続ではありません.

3 微分

今まで関数の極限についての導入をしてきたので, 今からはそれらを生かして微分を定義します.

定義 3.1

$f(x)$ が a で微分可能 $\underset{def}{\iff} \lim_{x\to a}\dfrac{f(x)-f(a)}{x-a}$ が存在する.この時この値を $f(x)$ の $x = a$ での微分係数といい, $f(a)'$ で表す.

(a, b) の各点で微分可能な時, $f(x)$ は (a, b) で微分可能と言う.

例

$$f(x) = x^2 \text{の時, これは } x = 0 \text{ で微分可能で, } f'(0) = \lim_{x\to 0}\frac{f(x)-f(0)}{x} = \lim_{x\to 0} x = 0$$

定義 3.2

関数 $f'(x)$ を, $x = a$ で $f'(a)$ をとる関数とする.

命題 3.3

$f(x)$ が $x = a$ で微分可能なら, $x = a$ で連続

証明

$f(x) = f(a) + f'(a)(x-a) + g(x)$ とおくと, $\lim_{x\to a} g(x) = 0$ なので,

$$\lim_{x\to a}(f(x) - f(a)) = \lim_{x\to a}(f'(a)(x-a) + g(x)) = 0\blacksquare$$

定理 3.4

$f(x)$ が $x = a$ で微分可能で, $f(a) \neq 0$ の時, $g(x) = \dfrac{1}{f(x)}$ が $x = a$ で微分可能で, $g'(a) = -\dfrac{f'(a)}{(f(a))^2}$

証明

$$g'(a) = \lim_{x\to a}\frac{g(x)-g(a)}{x-a} = \lim_{x\to a}\frac{\frac{1}{f(x)} - \frac{1}{f(a)}}{x-a} = \lim_{x\to a} -\frac{\frac{f(x)-f(a)}{x-a}}{f(x)f(a)} = -\frac{f'(a)}{(f(a))^2}(\because \lim_{x\to a} f(x) = f(a))\blacksquare$$

定理 3.5

$$f(a) = f(b) \text{ で}, f(x) \text{ が } [a,b] \text{ で連続}, (a,b) \text{ で微分可能ならば}, \text{ある}\delta \in (a,b) \text{ があって}, f'(\delta) = 0$$

証明

$$x_0 \in (a,b) \Rightarrow f(x_0) = f(a) \text{ の時}, \text{任意の値 } m \in (a,b) \text{ について}, f'(m) = 0 \text{ なので良い}.$$

$$\text{ある値 } x_0 \in (a,b) \text{ があって } f(x_0) \neq f(a) \text{ とする}. f(x_0) > f(a) \text{ とする } (< f(a) \text{ としても同様})$$

$$\text{この時}, f(x) \text{ は } [a,b] \text{ で連続なので}, \exists n \in (a,b), \forall \xi \in (a,b) \Rightarrow f(n) \geq f(\xi)(f(x) \text{ は } x = n \text{ で最大値をとる})$$

$$\text{この時}, x > n \text{ の時を考えると}, f'(n) = \lim_{x \to n} \frac{f(x) - f(n)}{x - n} \leqq 0(\because f(x) \leqq f(n))$$

$$\text{また } x < n \text{ の時を考えると}, f'(n) = \lim_{x \to n} \frac{f(x) - f(n)}{x - n} \geq 0(\because f(x) \leqq f(n)) \ \text{ 以上より}, f'(n) = 0 \blacksquare$$

定理 3.6

$$f(x), g(x) \text{ が } [a,b] \text{ で連続}, (a,b) \text{ で微分可能}, g(a) \neq g(b), \forall m \in [a,b], f'(m) \neq 0 \text{ または } g'(m) \neq 0 \text{ であるとする}.$$

$$\text{この時}, \exists \xi \in (a,b), \frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(\xi)}{g'(\xi)}$$

証明

$$F(x) = (g(b) - g(a))f(x) - (f(b) - f(a))g(x) \text{ とおくと}, F(a) = F(b).$$

$$\text{定理 3.5 より}, \exists \xi \in (a,b), F'(\xi) = 0, \text{ここで},$$

$$0 = F'(\xi) = \lim_{x \to \xi} \frac{F(x) - F(\xi)}{x - \xi} = (g(b) - g(a)) \lim_{x \to \xi} \frac{f(x) - f(\xi)}{x - \xi} - (f(b) - f(a)) \lim_{x \to \xi} \frac{g(x) - g(\xi)}{x - \xi} = (g(b) - g(a))f'(\xi) - (f(b) - f(a))f'(\xi)$$

$$\text{ここで } g'(\xi) = 0 \text{ とすると}, f'(\xi) \neq 0 \text{ より}, g(a) - g(b) \neq 0 \text{ より } (\text{左辺}) \neq 0, (\text{右辺}) = 0 \text{ より矛盾}.$$

$$\text{以上より両辺を } (g(b) - g(a))g'(\xi) \text{ で割ることが出来て}, \frac{f'(\xi)}{g'(\xi)} = \frac{f(b) - f(a)}{g(b) - g(a)} \blacksquare$$

4 ロピタルの定理

定理 4.1

1. $f(a) = g(a) = 0$ かつ, $\exists \delta > 0, 0 < |x - a| < \delta \Rightarrow f(x) \neq 0, g(x) \neq 0$
2. $\lim_{x \to a} f(x) = \infty, \lim_{x \to a} g(x) = \infty$

1 と 2 のどちらかが成り立っていて, かつ

$$\exists \epsilon_1 > 0, \exists \epsilon_2 > 0, 0 < |x - a| < \epsilon_1 \Rightarrow f(x) \text{ は微分可能}, 0 < |x - a| < \epsilon_2 \Rightarrow g(x) \text{ は微分可能}$$

$$\text{さらに}, \lim_{x \to a} \frac{f'(x)}{g'(x)} \text{の値が存在する時}, \lim_{x \to a} \frac{f(x)}{g(x)} = \lim_{x \to a} \frac{f'(x)}{g'(x)}$$

証明　$min(\delta, \epsilon_1, \epsilon_2) = \epsilon_0$ とする.

$$1.\ \ 0 < |x-a| < \epsilon_0 \Rightarrow f(x) \neq 0, g(x) \neq 0, f(x), g(x) \text{ は共に微分可能}$$

$$\text{よって}, \forall\epsilon \in (a, a+\epsilon_0) \Rightarrow g(\epsilon) \neq g(a) = 0, [a, \epsilon] \text{ で } f(x), g(x) \text{ は連続}, (a, a+\epsilon) \text{ で微分可能}$$

$$\text{よって定理 3.6 より}, \exists\xi \in (a, \epsilon) \text{ があって}, \frac{f(\epsilon)-f(a)}{g(\epsilon)-g(a)} = \frac{f'(\xi)}{g'(\xi)} \Rightarrow \frac{f(\epsilon)}{g(\epsilon)} = \frac{f'(\xi)}{g'(\xi)}$$

$$\text{同様に}\epsilon \in (a, a+\epsilon_0) \text{ の時も同様にして } \exists\xi \in (a, \epsilon), \frac{f(\epsilon)}{g(\epsilon)} = \frac{f'(\xi)}{g'(\xi)}$$

$$\text{ここで}\epsilon \to a \Rightarrow \xi \to a \text{ より}, \lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)} \quad \blacksquare$$

$$2. F(x) := \frac{1}{f(x)}(x \neq a)\ \ 0(x = a)\quad G(x) := \frac{1}{g(x)}(x \neq a)\ \ 0(x = a) \text{ とする}$$

$$\text{すると}, 0 < |x-a| < \epsilon_0 \Rightarrow F(x) \neq 0, G(x) \neq 0, F(x), G(x) \text{ は共に微分可能 } (\because \text{ 定理 3.4})$$

$$\text{よって 1.を適用することができて}, \lim_{x\to a} \frac{F(x)}{G(x)} = \lim_{x\to a} \frac{F'(x)}{G'(x)}$$

$$\text{整理して}, \lim_{x\to a} \frac{g(x)}{f(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)} \cdot \frac{(g(x))^2}{(f(x))^2}, \text{両辺に} \lim_{x\to a} \frac{(f(x))^2}{(g(x))^2} \text{を掛けて} \lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)} \blacksquare$$

5　あとがき

頭の中では単純なことだと思っていましたが, いざやってみると極限の定義, 微分の定義からなんやらで結構複雑になってしまいました. 特に極限の定義についてはなかなか初めて見る人にとっては理解しがたいかもしれません, そこは私の力不足であり, 申し訳ないです. さて, 私がこの記事を書こうと思った理由は, ロピタルの定理の形式が非常に美しく感じたからです. そしてゼミでやってる内容で証明することができると分かった時に, これを部誌にすることに決めました. 実は, このロピタルの公式はかなり実用性があり, 大学入試などの高校数学の極限を求める問題では非常に汎用性が高いです. これで答えだけは一発で出るなんてこともよくあります. これを読んでいる読者には,

$$f(a) = g(a) = 0 \text{ または} \lim_{x\to a} f(x) = \infty, \lim_{x\to a} g(x) = \infty \text{ ならば} \lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}$$

(多項式関数は全て連続や微分可能などのロピタルの定理を使用する上で必要な条件を満たすので入試などに出る関数には基本的に適用できます。)

という式は是非覚えてほしいと思います. それでは, ここまで読んでいただき, ありがとうございました.

6　参考文献

笠原 晧司 著　『微分積分学』(サイエンス社)

$$\lim_{x\to\infty}(1+\frac{1}{x})^x = e \text{ の証明}$$

高校 1 年 4 組 15 番　黒田直樹

1　はじめに

本日は数学研究部にお越しいただきありがとうございます. この記事では, 去年書いた e(ネイピア数) に関するものを訂正 (というか構成を一新) し, 論理の飛躍した部分をなくし, 微分積分の面から e を考え直し書いていきます. 微分積分の簡単な知識があれば読むことが出来ます.

2　準備

まずここで使う記号の導入をします.$a := b$ で a を b(に等しいもの) として定義するという意味です.

定義 2.1　$\log x := \int_1^x \frac{1}{t}dt(x>0)$ とし,$\log x$ を自然対数という

命題 2.2　$\log x$ は $x>0$ の時, 微分可能で単調増加である.

証明　定義 2.1 より自明に $(\log x)' = \frac{1}{x}\ (x>0)$ であり, また $\frac{1}{t}>0(t>0)$ なことから,
$\int_b^a \frac{1}{t}dt > 0(a>0, b>0, a>b)$. よって $a>b \Rightarrow \int_1^a \frac{1}{t}dt - \int_1^b \frac{1}{t}dt = \int_b^a \frac{1}{t}dt > 0 \Rightarrow \log a > \log b$　■

命題 2.3

$$\log ab = \log a + \log b(a>0, b>0)$$

証明　$a>0, b>0$ に対して
$\log ab - \log a = \int_1^{ab}\frac{1}{t}dt - \int_1^a \frac{1}{t}dt = \int_a^{ab}\frac{1}{t}dt = \int_1^b \frac{1}{ax}\frac{dt}{dx}dt(\because t=ax$ で置換$) = \int_1^b \frac{1}{ax}adx = \int_1^b \frac{1}{x}dx = \log b$

よって　　$\log ab = \log a + \log b$■

定理 2.4（中間値の定理）

$f(x)$ が $a \leqq x \leqq b$ で連続ならば, $f(a), f(b)$ の間の任意の値 k について, $f(c)=k$ となる a 以上 b 以下の値 c が存在する

証明　有名な定理なので省略します

命題 2.5

$\log e = 1$ となる数 e がただ一つ存在する.この数 e をネイピア数という.

証明　まず, 定義より自明に $\log 1 = 0, a>1 \Rightarrow \log a > 0(\because$ 命題 2.2)

命題 2.3 より自然数 n について $\log a^n = \log a^{n-1} + \log a = \cdots = n \log a$ すると,$a > 1$ のとき,

$$\lim_{n\to\infty} \log a^n = \lim_{n\to\infty} n \log a = \infty \quad \lim_{n\to\infty} a^n = \infty$$

よってこの二つと $\log x$ の単調増加性から,

$$\lim_{x\to\infty} \log x = \infty$$

が得られる.$0 < 1 < \infty$ なので, 定理 2.4 より $1 < e < \infty$ となる数 e で $\log e = 1$ となるようなものが存在する.また命題 2.2 より $\log a = \log b \Rightarrow a = b$ より, このような数 e は高々一つしかない. ■

命題 2.6

$$\lim_{x\to\infty} x \log(1 + \frac{1}{x}) = 1$$

証明 x を $\frac{1}{h}$ に置き換えると,$x \to \infty$ で $h \to +0$ であることに注意すると,

$$x \log(1 + \frac{1}{x}) = \frac{\log(1+h)}{h} = \frac{\log(1+h) - \log 1}{h} (\because \log 1 = 0)$$

これは $h \to +0$ で $\log x$ の x=1 での微分係数に等しくなる.$(\log x)' = \frac{1}{x}$ なので,

$$\lim_{x\to\infty} x \log(1 + \frac{1}{x}) = \frac{1}{1} = 1 \blacksquare$$

これで, 必要なことは終わりました.

3 指数関数

定義 3.1

$\log x$ は狭義単調増加なので, 逆関数を定義できる.それを e^x とする.つまり,$y = e^x \underset{def}{\Longleftrightarrow} x = \log y$ とする.

命題 3.2

$$e^x \text{は微分可能で}, (e^x)' = e^x$$

証明 逆関数の微分の公式より,$y = e^x$ とすると,

$$\frac{dy}{dx} = \frac{1}{\frac{d}{dy}\log y} = \frac{1}{\frac{1}{y}} = y = e^x \blacksquare$$

命題 3.3

$$a^x := e^{x \log a}$$

定理 3.4

$$1 \quad a^0 = 1$$

$$2 \quad a^1 = a$$

$$3 \quad a^x \cdot a^y = a^{x+y}$$

証明

$$1\quad a^0 = e^0, \text{ここで} \log 1 = 0 \text{ より } e^0 = 1, \text{よって } a^0 = 1$$

$$2\quad a^1 = e^{\log a} = a$$

3　$a^x = m, a^y = n$ とおくと,$m = a^x = e^{x \log a}$ より,$x \log a = \log m$,
同様にして $y \log a = \log n$, すると　$\log mn = \log m + \log n = (x + y) \log a$.
よって,$a^x \cdot a^y = e^{(x+y)\log a} = a^{x+y}$■

よって, これで定義した a^x によって,a の実数乗をうまく定義できることがわかります. これにより実数乗が定義できました. また

$$(a^x)' = (e^{x \log a})' = e^{x \log a} \cdot \log a = a^x \log a$$

より微分ができるので, この関数も連続であることが分かりました.

命題 3.5

$$\lim_{x\to\infty} (1 + \frac{1}{x})^x = e$$

証明

$$(1 + \frac{1}{x})^x = e^{x \log (1+\frac{1}{x})} \to e \qquad (x \to \infty)(\because \text{命題 } 2.6)■$$

4　あとがき

1. $\lim_{x\to\infty} (1 + \frac{1}{x})^x = e$
2. $\lim_{h\to 0} \frac{e^h - 1}{h} = 1$
3. $\log x = \log_e x$(但し, 左辺は定義 2.1 で定めたもの, 右は e を底とした対数関数)

この三つは同値関係で結ばれており, 去年の部誌では 2⇒ 1,3　今回のこの部誌では,3⇒ 1 を示したことになります (命題 2.3 から $\log x$ が対数関数であることがわかり,3 の式が成り立つ.) ともかく, 論理展開が滅茶苦茶だった去年と比べると大分ましなものができたと思っています. 最後に, ここまで読んでいただき, ありがとうございました

5　参考文献

笠原 晧司 著　『微分積分学』(サイエンス社)

位相と収束

高校2年1組42番 千綿啓暉

1. はじめに

本日は灘校文化祭、および数学研究部にお越しいただき、まことにありがとうございます。洗練されたものには程遠いと思われますが、目を通していただければ幸いです。

2. 準備

定義 2.1　順序, 順序集合

集合 A における関係 $\leqq$ が以下の3つをみたすとき、$\leqq$ を A における順序という。

(1) $\forall a \in A,\quad a \leqq a$

(2) $a, b \in A,\ a \leqq b,\ b \leqq a \Rightarrow a = b$

(3) $a, b, c \in A,\ a \leqq b,\ b \leqq c \Rightarrow a \leqq c$

この集合 A と順序 $\leqq$ の組 $(A, \leqq)$ を順序集合という。(順序集合 $(A, \leqq)$ を略して A と書くこともある。)

順序集合 A と $a, b \in A$ に対し、

$a \leqq b$ ($b \geqq a$ ともかく) のとき、a は b 以下である、または b は a 以上であるという。

$a \leqq b$ かつ $a \neq b$ のとき、$a < b$ ($b > a$ ともかく) で表し、a は b より小さい、または b は a より大きいという。

定義 2.2　最大元, 最小元

順序集合 A, $a \in A$ に対し、

$\forall x \in A,\ x \leqq a$ が成立するとき、a を A の最大元

$\forall x \in A,\ x \geqq a$ が成立するとき、a を A の最小元

という。

命題 1

順序集合 A に最大元(最小元)が存在するならば、それは一意である。

証明

a, a' がともに A の最大元であるならば、

$a \leqq a'$ かつ $a' \leqq a$ ゆえに $a = a'$

同様にして、最小元も一意。 ■

定義 2.3 族

ある集合 Λ からある集合 A への写像 a を、A の元の族という。

各 $\lambda \in \Lambda$ の a による像 $a(\lambda)$ を a_λ とかき、a を $(a_\lambda)_{\lambda \in \Lambda}$ で表す。

各 $\lambda \in \Lambda$ においてとる値が集合 A_λ となるとき $(A_\lambda)_{\lambda \in \Lambda}$ を集合族という。

集合族 $(A_\lambda)_{\lambda \in \Lambda}$ の和集合を、

$$\bigcup_{\lambda \in \Lambda} A_\lambda := \{ x \mid \exists \lambda \in \Lambda, \ x \in A_\lambda \}$$

共通部分を、

$$\bigcap_{\lambda \in \Lambda} A_\lambda := \{ x \mid \forall \lambda \in \Lambda, \ x \in A_\lambda \}$$

で定義する。

定義 2.4　位相

ϕ で空集合，$\mathcal{P}(X)$ で集合 X の部分集合全体の集合を表す。

集合 $S\ (\neq \phi)$，$\mathcal{O} \subset \mathcal{P}(S)$ に対し，

$\mathcal{O}$ が以下の3つをみたすとき，$\mathcal{O}$ は S の位相であるという．

(1) $\phi,\ S \in \mathcal{O}$

(2) $O_1, O_2 \in \mathcal{O} \Rightarrow O_1 \cap O_2 \in \mathcal{O}$

(3) $\mathcal{O}$ の元からなる集合族 $(O_\lambda)_{\lambda \in \Lambda}$ に対し

$$\bigcup_{\lambda \in \Lambda} O_\lambda \in \mathcal{O}$$

この S と $\mathcal{O}$ の組 $(S, \mathcal{O})$ を位相空間という。

(位相空間 $(S, \mathcal{O})$ を略して S と書くこともある。)

定義 2.5　開集合，閉集合

位相空間 S と $M \subset S$ に対し．M^c で M の S に対する補集合を表す．

M が開集合である $\overset{def}{\Leftrightarrow}$ $M \in \mathcal{O}$

M が閉集合である $\overset{def}{\Leftrightarrow}$ $M^c \in \mathcal{O}$

として，定義する．

定義 2.6　開核，閉包

位相空間 S と $M \subset S$ に対し．

M' が M の開核であることを

M' が M に含まれる最大の開集合であることと定める．

M' が M の閉包であることを

M' が M を含む最小の閉集合であることと定める．

ここでいう最大，最小というのは

$M, N \subset S$ に対し．$M \leq N \Leftrightarrow M \subset N$ として

Sに順序を定めたときに、それにおいて最大元、最小元であることを意味する。
開核の存在については、$\forall M \subset S$ に対して、Mに含まれる開集合すべての和集合は定義 2.4 の条件 (3) より、また開集合であり、Mに含まれる開集合の最大のものである。
閉包の存在については、A_λを閉集合とすると、集合族 $(A_\lambda)_{\lambda \in \Lambda}$ について、定義 2.4 の (3) より、

$$\bigcup_{\lambda \in \Lambda} A_\lambda^c \in \mathcal{O}$$

$$\bigcup_{\lambda \in \Lambda} A_\lambda^c = \left(\bigcap_{\lambda \in \Lambda} A_\lambda\right)^c \quad \text{であるから}$$

$\bigcap_{\lambda \in \Lambda} A_\lambda$ は閉集合であることがわかる
$\forall M \subset S$ に対し、Mを含む閉集合すべての共通部分は、また閉集合でMを含む最小の閉集合となる。
これは、任意のSの部分集合に開核、閉包が存在することを示している。
以降、Mの開核を M°、閉包を $\overline{M}$ で表す。

命題、2

位相空間 S、$M \subset S$ に対し、
Mが開集合である $\Leftrightarrow$ $M = M^\circ$
Mが閉集合である $\Leftrightarrow$ $M = \overline{M}$

これは定義より自明である。

命題、3

位相空間 S、$M \subset S$ に対し、
$\overline{M^c} = (M^\circ)^c$

証明.

開核の定義より $M^\circ \subset M$

ゆえに $M^c \subset (M^\circ)^c$

M° は開集合だから, $(M^\circ)^c$ は閉集合.

A を $A \supset M^c$ なる閉集合とすると

A^c は開集合で $A^c \subset M$

ゆえに $A^c \subset M^\circ$ $\quad\therefore\ A \supset (M^\circ)^c$

したがって $(M^\circ)^c$ は M^c を含む最小の閉集合,

$\therefore\ \overline{M^c} = (M^\circ)^c$ ■

定義 2.7 内点, 触点,

位相空間 S, $M \subset S$ に対し

M° に属する点を M の内点,

$\overline{M}$ に属する点を M の触点

という.

定義 2.8 近傍

位相空間 $(S, \mathcal{O})$, $x \in S$ に対し.

$V \subset S$ が x の近傍であるとは

$x \in V^\circ$ が成立することと定義する.

このことは, $\exists O \in \mathcal{O}$, $x \in O$, $O \subset V$ と同等である。

また, x の近傍全体の集合を $V(x)$ で表す.

命題 4

位相空間 S, $M \subset S$ に対し.

$x \in \overline{M} \Leftrightarrow \forall V \in V(x),\ M \cap V \neq \phi$

証明

$x \in \overline{M}$ ならば

$\exists V \in \mathcal{V}(x)$, $M \cap V = \phi$ と仮定すると、

そのような V に対し、 $x \in V^\circ$

ゆえに $x \notin (V^\circ)^c$

$(V^\circ)^c$ は閉集合であり、

$M \cap V = \phi$ より $M \subset V^c$

$V^\circ \subset V$ より $V^c \subset (V^\circ)^c$ だから $M \subset (V^\circ)^c$

よって $\overline{M} \subset (V^\circ)^c$

しかし、 $x \in \overline{M}$, $x \notin (V^\circ)^c$ であるから矛盾。

したがって $\forall V \in \mathcal{V}(x)$, $M \cap V \neq \phi$

逆を示す。

$\forall V \in \mathcal{V}(x)$, $M \cap V \neq \phi$ ならば

$x \notin \overline{M}$ と仮定すると、 $x \in (\overline{M})^c$

$(\overline{M})^c$ は開集合より $(\overline{M})^c \in \mathcal{V}(x)$

よって $M \cap (\overline{M})^c \neq \phi$ であるが、

$M \subset \overline{M}$ より $(\overline{M})^c \subset M^c$.

よって $M \cap (\overline{M})^c \subset M \cap M^c = \phi$.

これは矛盾であるから $x \in \overline{M}$ である。 ■

3. 有向点列の収束

定義 3.1 有向集合

順序集合 A において、

$\forall \alpha, \beta \in A$, $\exists \gamma \in A$, $\alpha \leqq \gamma$, $\beta \leqq \gamma$

が成立するとき A を有向集合という。

定義 3.2 有向点列

位相空間 S, 有向集合 A に対し、

S の元の族 $(a_\alpha)_{\alpha \in A}$ を有向点列という。

定義 3.3 有向点列の収束

位相空間 S，有向集合 A において

S の有向点列 $(a_\alpha)_{\alpha\in A}$ が $a\in S$ に収束するとは、

$\forall V\in \mathcal{V}(a)$，$\exists \alpha_0\in A$，$\forall \alpha\geqq\alpha_0$，$\alpha\in A$，$a_\alpha\in V$

が成立することと定義する。

このことを

$\lim_A a_\alpha = a$ または $a_\alpha(A)\to a$ とかき、

これを略して

$\lim a_\alpha = a$ または $a_\alpha\to a$ ともかく。

またこのとき，a を $(a_\alpha)_{\alpha\in A}$ の極限という。

定理．1

S を位相空間とする。

$M\subset S$ が閉集合 $\Leftrightarrow$ M の有向点列の極限となるような S の元すべてが M に属する。

補題

位相空間 S，$M\subset S$，$a\in S$ に対し

$a\in \overline{M}$ $\Leftrightarrow$ $a_\alpha\to a$ となるような M の有向点列 $(a_\alpha)_{\alpha\in A}$ が存在する。

補題の証明

$\mathcal{V}(a)$ に次のように関係 $\leqq$ を定める。

$U, V\in\mathcal{V}(a)$ に対し

$$V\leqq U \Leftrightarrow V\supset U$$

これが順序であることは明らかである。

このとき $(\mathcal{V}(a), \leqq)$ は有向集合となることが次のようにしてわかる。

まず，$\forall U, V\in \mathcal{V}(a)$，$U\cap V\in\mathcal{V}(a)$

$\because$ $U, V\in\mathcal{V}(a)\Leftrightarrow a\in U^\circ, a\in V^\circ \Leftrightarrow a\in U^\circ\cap V^\circ$

No.

Date

$\mathcal{U}^{\circ} \cap V^{\circ}$は開集合で $\mathcal{U}^{\circ} \cap V^{\circ} \subset \mathcal{U} \cap V$

$\therefore \mathcal{U}^{\circ} \cap V^{\circ} \subset (\mathcal{U} \cap V)^{\circ}$

$\therefore a \in (\mathcal{U} \cap V)^{\circ}$ つまり, $\mathcal{U} \cap V \in V(a)$.

次に, $\mathcal{U} \cap V \subset \mathcal{U}$, $\mathcal{U} \cap V \subset V$ より.

$\mathcal{U} \leqq \mathcal{U} \cap V$, $V \leqq \mathcal{U} \cap V$.

したがって $(V(a), \leqq)$ が有向集合であることが示された.

$a \in \overline{M}$ ならば 命題4 より

$\forall V \in V(a)$, $M \cap V \neq \phi$

ここで, 有向点列 $(a_V)_{V \in V(a)}$ を次のように定める

$\forall V \in V(a)$, $a_V \in M \cap V$

このとき明らかに $a_V \to a$.

逆を示す.

$(a_\alpha)_{\alpha \in A}$ を M の有向点列とする.

$(a_\alpha)_{\alpha \in A}$ が a に収束するならば

$\forall V \in V(a)$, $\exists \alpha_0 \in A$, $\forall \alpha \geqq \alpha_0$, $\alpha \in A$, $a_\alpha \in V \cap M$

ゆえに $\forall V \in V(a)$, $V \cap M \neq \phi$

命題4 より $a \in \overline{M}$ ∎

定理1の証明

命題2 より Mが閉集合 $\Leftrightarrow$ $M = \overline{M}$

$M = \overline{M}$ のとき, 補題より, Mの有向点列の極限となるようなすべてのSの元が $\overline{M}$ に属する. つまり, M に属している.

逆に aを任意のある有向点列(M_α)の極限となるSの元とする. このとき補題より $a \in \overline{M}$ と同等である.

よって $a \in \overline{M} \Rightarrow a \in M$ が成り立つ

したがって $\overline{M} \subset M$ であるが, 閉包の定義より $M \subset \overline{M}$ であるから $M = \overline{M}$ ∎

この定理1から，有向点列に関する情報が与えられたときに，閉集合を特定することができることがわかる.

4. フィルター

定義 4.1 フィルター

集合 X において $\mathcal{F} \subset \mathcal{P}(X)$ が X 上のフィルターであるとは，$\mathcal{F}$ が以下の3つをみたすことをいう.

(1) $\phi \notin \mathcal{F}$

(2) $A \in \mathcal{F},\ A \subset A' \subset X \Rightarrow A' \in \mathcal{F}$

(3) $A, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F}$

定義 4.2 フィルターの収束

位相空間 S，S 上のフィルター $\mathcal{F}$ に対し，

$\mathcal{F}$ が $a \in S$ に収束するとは

$$V(a) \subset \mathcal{F}$$

が成立することである.

このことを $\lim \mathcal{F} = a$ とかく.

この a を $\mathcal{F}$ の極限という.

定理 2

位相空間 S に対し，

$M \subset S$ が閉集合 $\Leftrightarrow$ M を含む S 上のフィルターの極限となるような S の元すべてが M に属する.

補題.1

位相空間 S, $M \subset S$, $a \in S$ に対し.

$a \in M^\circ \iff a$ に収束する任意の S 上のフィルターが M を含む

補題1の証明

$a \in M^\circ \Rightarrow M \in V(a)$

a に収束する任意の S 上のフィルター $\mathcal{F}$ に対し.

$$V(a) \subset \mathcal{F}$$

$$\therefore \quad M \in \mathcal{F}.$$

逆を示す.

$V(a)$ がフ　フィルターとなることは以下のように確かめられる.

$\phi \notin V(a)$, $A \in V(a)$ かつ $A \subset A' \subset S \Rightarrow A' \in V(a)$ は明らか.

$$\begin{aligned} A, B \in V(a) &\Rightarrow a \in A^\circ,\ a \in B^\circ \\ &\Rightarrow a \in A^\circ \cap B^\circ \subset (A \cap B)^\circ \\ &\Rightarrow A \cap B \in V(a) \end{aligned}$$

ゆえに $M \in V(a) \iff a \in M^\circ$. ∎

補題.2

位相空間 S, $M \subset S$, $a \in S$ に対し.

$a \in \overline{M} \iff a$ に収束するある S 上のフィルターが M を含む.

補題2の証明

「$a \notin \overline{M} \iff a$ に収束する任意の S 上のフィルターが M を含まない」

を示せばよい.

$a \notin \overline{M} \iff a \in (\overline{M})^c$

$$(\overline{M})^c = (\overline{M^{cc}})^c = \{(M^c)^\circ\}^{cc} = (M^c)^\circ \quad \text{より.}$$

$a \notin \overline{M} \iff a \in (M^c)^\circ$

ここでは命題.3を用いた.

補題.1より

$a \in (M^c)^\circ \Leftrightarrow$ aに収束する任意のS上のフィルターがM^cを含む.

任意のフィルター$\mathcal{F}$に対し,

$A \in \mathcal{F} \Rightarrow A^c \notin \mathcal{F}$

なぜならば A, A^cが共に$\mathcal{F}$に属するならば

$A \cap A^c = \phi$ も $\mathcal{F}$に属するが,これは矛盾.

ゆえに

$a \in (M^c)^\circ \Leftrightarrow$ aに収束する任意のS上のフィルターがMを含まない.

よって示された ■

定理2の証明

Mが閉集合 $\Leftrightarrow M = \overline{M}$

$M = \overline{M}$のとき,aをMを含むS上のフィルターの極限とすると,

補題2より $a \in \overline{M} \Leftrightarrow a \in M$.

よって必要性が示された.

十分性を示す.

$a \in \overline{M}$ならば補題2より,aはMを含むあるS上のフィルターの極限となる.

ゆえに $a \in M$

よって $\overline{M} \subset M$, $M \subset \overline{M}$は明らか.

よって $M = \overline{M}$ ■

この定理2からは,フィルターの収束に関する情報が与えられたときに,閉集合を特定することができることがわかる.

No.

Date

定理1、2の結果は似ていて、有向点列とフィルターには深い関係がありそうである。

定理3

位相空間 S、S の有向点列 $(a_\alpha)_{\alpha \in A}$ に対し、

$\exists \alpha_0 \in A$, $\forall \alpha \geqq \alpha_0$, $\alpha \in A$, $a_\alpha \in F$ $(F \subset S)$.

なる F 全体を $\mathcal{F}$ とする。このとき $\mathcal{F}$ は S 上のフィルターであり、$a \in S$ に対し、

$$\lim \mathcal{F} = a \iff \lim a_\alpha = a.$$

証明。

$\mathcal{F}$ がフィルターであることを示す。

明らかに $\phi \notin \mathcal{F}$.

また $F \in \mathcal{F}$　$F \subset F' \subset S$ ならば $F' \in \mathcal{F}$ も明らかである。

$F_1, F_2 \in \mathcal{F}$ ならば

$\exists \alpha_0 \in A$, $\forall \alpha \geqq \alpha_0$, $\alpha \in A$, $a_\alpha \in F_1$

$\exists \alpha_0' \in A$, $\forall \alpha \geqq \alpha_0'$, $\alpha \in A$, $a_\alpha \in F_2$

ここで A は有向集合だから、

$\exists \beta \in A$, $\alpha_0 \leqq \beta$, $\alpha_0' \leqq \beta$.

ゆえに、$\forall \alpha \geqq \beta$, $a_\alpha \in F_1 \cap F_2$.

$\therefore$ $F_1 \cap F_2 \in \mathcal{F}$.

したがって $\mathcal{F}$ は S 上のフィルターである。

次に後半を示す。

$\lim \mathcal{F} = a \iff V(a) \subset \mathcal{F}$.

$\iff \forall V \in V(a)$ に対し、$\exists \alpha_0 \in A$, $\forall \alpha \geqq \alpha_0$, $\alpha \in A$, $a_\alpha \in V$.

$\iff \lim a_\alpha = a$.　■

5. フィルターによる位相の定義

定理.4

集合 X と X 上のフィルター $\mathcal{F}$ に対し、

集合系 $\mathcal{O}$ を以下のように定める.

(i) $\phi \in \mathcal{O}$

(ii) $O\ (\neq \phi) \in \mathcal{O} \Leftrightarrow O \in \mathcal{F}$

このように定めた $\mathcal{O}$ について以下の3つが成立する.

(1) $\phi, S \in \mathcal{O}$

(2) $O_1, O_2 \in \mathcal{O} \Rightarrow O_1 \cap O_2 \in \mathcal{O}$

(3) $\mathcal{O}$ の元から成る集合族 $(O_\lambda)_{\lambda\in\Lambda}$ に対し.

$\bigcup_{\lambda\in\Lambda} O_\lambda \in \mathcal{O}$

証明

$\phi \in \mathcal{O}$ は明らか.

$\forall F \in \mathcal{F}$ に対し. $F \subset X \subset X$ より $X \in \mathcal{F}$

次に、※ $O_1, O_2 \in \mathcal{O} \Leftrightarrow O_1, O_2 \in \mathcal{F}$

$\Rightarrow O_1 \cap O_2 \in \mathcal{F}$ ($\because$ フィルターの定義)

$\Leftrightarrow O_1 \cap O_2 \in \mathcal{O}$

最後に、※ $\forall\lambda \in \Lambda, O_\lambda \in \mathcal{O} \Leftrightarrow \forall\lambda\in\Lambda, O_\lambda \in \mathcal{F}$

$\forall\lambda\in\Lambda, O_\lambda \in \mathcal{F}$ で $O_\lambda \subset \bigcup_{\lambda\in\Lambda} O_\lambda \subset X$ より

$\bigcup_{\lambda\in\Lambda} O_\lambda \in \mathcal{O}$

ゆえに示された (※については最後のページへ) ■

この定理4によって、集合 X にあるフィルターを1つ与えたとき、それによって定められる上の $\mathcal{O}$ は定義2.4の位相がみたすべき3条件をみたしている. つまり、集合 X と集合系 $\mathcal{O}$ の組 $(X, \mathcal{O})$ は位相空間となる. したがって、集合 X に1つのフィルターを与えたとき、それによって位相を定義する

ことができることがわかる。

6. おわりに

位相による収束を知ったときに、開集合系、閉集合系、開核作用子、閉包作用子、近傍系などから位相を定めることができるのと同じように収束から位相を定めることもできるのではないかと思い、考えていたところ、フィルターを定めれば位相も定まるという結果に至りました。

この記事の中に誤りや、おかしなところがあればご指摘していただけると有難いです。自分の成長につなげられればと思う次第です。

目を通していただきありがとうございます。

参考文献

松坂和夫著「集合・位相入門」

※ O_1, O_2 のうちのいずれか一方が ϕ のときは明らかに成立し、ある $\lambda \in \Lambda$ に対し、$O_\lambda = \phi$ のときでも成立します。書き忘れていました。すみません。

フェルマーの最終定理 (n=3,4) に初等整数論で挑む

高校2年2組32番 大宮 一人

0 はじめに

本日は灘校文化祭及び数学研究部にお越しいただき、誠にありがとうございます。
Texが使えないので手書きです。また、字が下手である為読みにくいと思います。申し訳ありません。
今回は、みなさんご存知フェルマーの最終定理
『3以上の自然数※ n について、$a^n+b^n=c^n$ を満たす自然数 (a,b,c) の組が存在しない』
について、$n=3,4$ の時の証明を初等整数論を用いて行っていこうと思います。

1 $n=4$ の時

以下、特に断りのない場合、$a,b\in\mathbb{Z}\setminus\{0\}$ に対し (a,b) は a と b の最大公約数を意味するものとする。

1.1 $a^2+b^2=c^2$ の自然数解について

まず、$(a,b)=(b,c)=(c,a)=1$ としてよいことを示す。

<pf> a,b が共通の素因数 p を持つと仮定すると、c^2 も p の倍数であり
p が素数であることから c も p の倍数。この時 $\frac{a}{p},\frac{b}{p},\frac{c}{p}\in\mathbb{N}$ であり
$\left(\frac{a}{p}\right)^2+\left(\frac{b}{p}\right)^2=\left(\frac{c}{p}\right)^2$ である。これを繰り返すことで $(a,b)=1$ としてよい。
b,c、c,a についても同様。□

また、$c^2-b^2=a^2>0$、$c>0$、$b>0$ より $c>b$ である。
この時 $a^2+b^2=c^2 \iff a^2=(c+b)(c-b)$

(i) $c+b$、$c-b$ が共通な素因数 α を持つ時
$c+b=\alpha k$、$c-b=\alpha l$ を満たす $k,l\in\mathbb{N}$ $(k>l)$ が存在する。
この時 $c=\frac{\alpha(k+l)}{2}$、$b=\frac{\alpha(k-l)}{2}$ である。

(ア) α が奇数の時
b,c が奇数であることから、$k+l$、$k-l$ が共に偶数であることが必要であり、この時 b,c は共通の素因数 α を持つ。従ってこの場合は考慮しなくてもよい。

(イ) α が偶数、つまり $\alpha=2$ の時
$c=k+l$、$b=k-l$ であり、この時 $a=2\sqrt{kl}$ より kl は平方数。
k,l が共通の素因数 p を持つと仮定すると b,c は共通の素因数 p を持つので、$(k,l)=1$ としてよい。この時 k,l は互いに素な平方数であり、
$(a,b,c)=(2xy,\ x^2-y^2,\ x^2+y^2)$ $((x,y)=1)$ と表される。

(ii) $(c+b,\ c-b)=1$ の時
a^2 が平方数であることから、$c+b$、$c-b$ は互いに素な平方数でなければならず、
$(x_1,y_1)=1$ を満たす $x_1,y_1\in\mathbb{N}$ を用いて $c+b=x_1^2$、$c-b=y_1^2$ と表される。
この時 $(a,b,c)=\left(x_1y_1,\ \frac{x_1^2-y_1^2}{2},\ \frac{x_1^2+y_1^2}{2}\right)$ である。

※「自然数」は「1以上の整数」の意味で用いている。

1.1 (ii) $(x_1, y_1) = 1$、$\frac{x_1^2 - y_1^2}{2} \in \mathbb{N}$ より x_1, y_1 は奇数である。

従って $x_1 = X + Y$、$y_1 = X - Y$ を満たす $X, Y \in \mathbb{N}$ $(X > Y)$ が存在し

この時 $(a, b, c) = (X^2 - Y^2, 2XY, X^2 + Y^2)$ と表される。

以上より、$a^2 + b^2 = c^2$ の自然数解の組 (a, b, c) は異なる2自然数

x, y $(x > y)$ を用いて $(a, b, c) = (2xy, x^2 - y^2, x^2 + y^2)$ と表される。

1.2 $a^4 + b^4 = c^4$ を満たす自然数の組の不存在証明

$a^4 + b^4 = c'^2$ を満たす自然数解の組 (a, b, c') が存在しないことを

示せば十分である。$a^2 = X$、$b^2 = Y$ とおくと 1.1 より

$X = 2xy$、$Y = x^2 - y^2$、$c' = x^2 + y^2$ $(x, y \in \mathbb{N}, x > y)$ と表される

補題 1.2.1 $(X, Y) = (Y, c') = (c', X) = 1$ としてよい。

<pr> Y, c' が共通素因数 α を持つとすると $X^2 = c'^2 - Y^2$ より X^2 は α の倍数

であり、α は素数なので X は α の倍数。この時 c' は α^2 の倍数であり、

$\frac{X}{\alpha}, \frac{Y}{\alpha}, \frac{c'}{\alpha^2} \in \mathbb{N}$、$\left(\frac{X}{\alpha}\right)^2 + \left(\frac{Y}{\alpha}\right)^2 = \frac{c'}{\alpha^2}$ である。

これを繰り返すことで $(Y, c') = 1$ としてよい。X, Y、c', X についても同様 $\blacksquare$

以下 $(X, Y) = (Y, c') = (c', X) = 1$ とする

補題 1.2.2 $(x, y) = 1$ である

<pr> x, y が共通の素因数 p を持つと仮定すると、$X = 2xy$ $Y = x^2 - y^2$

より X, Y は共に p の倍数。これは $(X, Y) = 1$ に矛盾する。従って $(x, y) = 1$ $\blacksquare$

補題 1.2.3 x は奇数 y は偶数

<pr> X が平方数なので $2xy$ は平方数であり、2は素数であることから、x, y の

少なくとも一方は偶数。$(x, y) = 1$ より偶数であるのは片方のみである。

x が偶数であるとすると $x \equiv 0, 2 \pmod 4$、$y \equiv \pm 1 \pmod 4$ であり、この時

$Y \equiv x^2 - y^2 \equiv 0 - 1 \equiv -1 \pmod 4$ となるが、これは Y が平方数であること

に矛盾する。よって x は奇数、y は偶数 $\blacksquare$

よって $(x, y) = 1$、$Y = x^2 - y^2$ より $(\gamma, \delta) = 1$ なる $\gamma, \delta \in \mathbb{N}$ $(\gamma > \delta)$ を用いて

$Y = (\gamma^2 - \delta^2)^2$ $x = \gamma^2 + \delta^2$、$y = 2\gamma\delta$ と表せる。

この時、$x = \gamma^2 + \delta^2$、$(\gamma, \delta) = 1$ より 今までの議論と同様に $(x, \gamma) = (\gamma, \delta) = (\delta, x) = 1$

$X^2 = 2xy = 4x\gamma\delta$ なので、x, γ, δ は全て平方数である。

$c' - X = x^2 + y^2 - 2xy = (x - y)^2 > 0$ より $c' > X$、$X > x$ ($\because$ $y > 0$ より $2y > 0$)

であるので $c' > x$

従って $X^2 + Y^2 = c'^2$ を満たす X, Y が平方数で c'^2 が最小の自然数の組 (X, Y, c'^2) をとった時、

それよりも c'^2 の値が小さい組 (γ, δ, x) が存在し c'^2 の最小性に矛盾する。

よって、$a^4 + b^4 = c'^2$ を満たす自然数の組 (a, b, c') は存在しない。つまり $a^4 + b^4 = c^4$ を満たす

自然数の組 (a, b, c) は存在しない $\blacksquare$

2 $n=7$ の時

2.1 $\mathbb{Z}[w]$ について

$w = \dfrac{-1+\sqrt{7}i}{2}$ とする．この時 $w^3=1$、$w^2+w+1=0$ が成り立つ．

以下 $\mathbb{Z}[w] := \{a+bw \mid a,b \in \mathbb{Z}\}$ が一意分解環であることを示す

Def 環
集合 A に二つの演算 $+$ と $\times$ が定義されており、以下の性質を満たす時、A を環という
(1) $^\forall a, b \in A \quad a+b = b+a$
(2) $^\forall a, b, c \in A \quad (ab)c = a(bc)$
(3) $^\forall a, b, c \in A \quad a(b+c) = ab+ac$
(4) $^\forall a, b \in A \quad ab = ba$
(5) 乗法について単位元 1 がある．$1 \cdot a = a \cdot 1 = a$

$\mathbb{Z}[w]$ は上記の性質を全て満たすので環である

Def 整域
A が環であり $^\forall a, b \in A \setminus \{0\}$、$ab \neq 0$ となる時 A を整域という

$\mathbb{Z}[w]$ は上記の性質を満たすので整域である。

Def ユークリッド環
整域 A が以下の条件を満たす時、ユークリッド環という。
「写像 $d : A \setminus \{0\} \to \mathbb{N}$ があり、$a, b \in A$ で $b \neq 0$ ならば
$q, r \in A$ があり $a = qb + r$ で $r=0$ 又は $d(r) < d(b)$ となる」

要するに、ユークリッド環とは割り算の余りの概念がある環であり、一般にユークリッド環であるものは一意分解環 (UFD) であることが知られている．

以下、$\mathbb{Z}[w]$ がユークリッド環であり、従って一意分解環であることを示す。

<pf> $\alpha = x + yw$ ($x, y \in \mathbb{Q}$) に対し、$d(\alpha) = |\alpha| = (x-\frac{y}{2})^2 + (\frac{\sqrt{7}y}{2})^2 = x^2 - xy + y^2$

とすると、d は 0 以外の $\mathbb{Z}[w]$ の元を自然数に写す写像である ($\because |\alpha| > 0$)

$a, b \in A$ をとると $\frac{a}{b} = x_1 + y_1 w$ ($x_1, y_1 \in \mathbb{Q}$) である

(i) $\frac{a}{b} \in A$ の時　$q = \frac{a}{b}$、$r=0$ とするとこれは $a = qb + r$ を満たす．

(ii) $\frac{a}{b} \notin A$ の時　$|c - x_1|$、$|d - y_1|$ が最小となる様な $c, d \in \mathbb{Z}$ をとると

$|c-x_1| \leqq \frac{1}{2}$、$|d-y_1| \leqq \frac{1}{2}$　$x_2 = c - x_1$、$y_2 = d - y_1$ とすると $x_2, y_2 \in \mathbb{Q}$

$|x_2 + y_2 w| = x_2^2 - x_2 y_2 + y_2^2$

$\leqq |x_2|^2 + |x_2||y_2| + |y_2|^2 \leqq (\frac{1}{2})^2 + \frac{1}{2} \cdot \frac{1}{2} + (\frac{1}{2})^2 = \frac{3}{4} < 1$

従って $q = c + dw$、$r = a - bq$ とすると $q, r \in A$、$a = qb + r$ で

$\frac{|r|}{|b|} = |\frac{r}{b}| = |\frac{a}{b} - q| = |(x_1 + y_1 w) - (c + dw)| = |-(x_2 + y_2 w)| < 1$

より $|r| < |b|$　$\therefore d(r) < d(b)$

よって $\mathbb{Z}[w]$ はユークリッド環であり、従って一意分解環である．▨

2　2.2 準備A（定義）

Def 約元・倍元

Aを整域、$a, b \in A$、$a \neq 0$とする。$c \in A$があり、$b = ac$となるなら、bはaの倍元、aはbの約元という。この時 $a \mid b$ と書く。

$A \subset \mathbb{C}$などの場合には倍数、約数といった用語を用いることが多い。

$\mathbb{Z}[\omega] \subset \mathbb{C}$なので今回はこちらの表記を用いる。

Def 公約元、最大公約元

Aを一意分解環、$a, b \in A \setminus \{0\}$とする。$c \mid a, b$ なる c は a, b の公約元という。

cがa, bの公約元で dもa, bの公約元なら $d \mid c$ となる時 cをa, bの最大公約元という

こちらも同様に公約数、最大公約数という表記を用いる。また cがa, bの最大公約数であることを $(a, b) = c$ と表記する。

Def 合同

Aを整域、$m \in A \setminus \{0\}$とする。$a, b \in A$であり $m \mid a - b$ であるなら、$a \equiv b \pmod{m}$ と書き、a, bはmを法として合同という。

Def ※$\mathbb{Z}[\omega]$のオーダー

pを$\mathbb{Z}[\omega]$の素元とする。$a \in \mathbb{Z}[\omega]$に対し、$\frac{a}{p^n} \in \mathbb{Z}[\omega]$、$\frac{a}{p^{n+1}} \notin \mathbb{Z}[\omega]$ となる非負整数nを $\mathrm{ord}_p(a)$ と書き、aのpに関するオーダーという

便宜上 $\mathrm{ord}_p(0) = \infty$ とする。また上の定義より下の(1),(2)が成立することは容易に示せる。

(1) $a, b \in \mathbb{Z}[\omega]$ なら $\mathrm{ord}_p(ab) = \mathrm{ord}_p a + \mathrm{ord}_p b$

(2) $a, b \in \mathbb{Z}[\omega]$ で $\mathrm{ord}_p a \neq \mathrm{ord}_p b$ なら

$$\mathrm{ord}_p(a+b) = \min\{\mathrm{ord}_p a, \mathrm{ord}_p b\}$$

2.3 準備B（$\mathbb{Z}[\omega]$の性質）

補題2.3.1　単元は ± 1、$\pm\omega$、$\pm\omega^2$ のみである。

<Pf> $(a + b\omega)(c + d\omega) = 1$ を満たす $a, b, c, d \in \mathbb{Z}$ について

$$ac + (bc + ad)\omega + bd\omega^2 = 1$$

$$ac + (bc + ad)\omega + bd(-1 - \omega) = 1$$

$$(ac - bd) + (bc + ad - bd)\omega = 1$$

$$\begin{cases} ac - bd = 1 & \cdots ① \\ bc + ad - bd = 0 & \cdots ② \end{cases}$$

①より $bc \cdot ad - b^2d^2 = bd$　$\therefore bc \cdot ad = b^2d^2 + bd$

②より $bc + ad = bd$

よって bc, ad を解に持つ2次方程式の1つは

$$x^2 - bdx + b^2d^2 + bd = 0 \quad \cdots (*)$$

※厳密な定義は多少異なるが、$\mathbb{Z}[\omega]$に限定すると本質的には大差ないので、今回はこの定義を採用する

2　2.3　補題 2.3.1 <pf>　この2次方程式の判別式 D について

$D = (bd)^2 - 4(b^2d^2 + bd)$

$\quad = -3(bd + \frac{2}{3})^2 + \frac{4}{3}$

これが 0 以上となるのは $bd = 0, -1$ の時のみ

$bd = -1$ の時　(*) は $x^2 + x = 0$ となり　$x = 0, -1$

つまり $(bc, ad) = (0, -1), (-1, 0)$

$\therefore (a, b, c, d) = (0, 1, -1, -1), (1, 1, 0, -1)$

$(-1, -1, 0, 1), (0, -1, 1, 1)$

この時　$a+b\omega,\ c+d\omega$ は $\pm\omega,\ \pm\omega^2$

$bd = 0$ の時　$b = 0$ とすると　①より $ac = 1$　$\therefore a = c = \pm 1$

この時 ②より $d = 0$ であり　$a+b\omega,\ c+d\omega$ は ± 1 である

よって 単元は $\pm 1, \pm\omega, \pm\omega^2$ のみである。□

補題 2.3.2　$\omega - 1$ は素元である。

<pf>　$\omega - 1$ が単元を含まない2積に分解できないことを示せばよい。

$\omega - 1 = (a+b\omega)(c+d\omega)$ を満たす $a, b, c, d \in \mathbb{Z}$ について

$$\begin{cases} ac - bd = -1 & \cdots ③ \\ bc + ad - bd = 1 & \cdots ④ \end{cases}$$

③より $bc \cdot ad - b^2d^2 = -bd$　$\therefore bc \cdot ad = b^2d^2 - bd$

④より $bc + ad = bd + 1$

従って bc, ad を解に持つ2次方程式の1つは

$t^2 - (bd+1)t + b^2d^2 - bd = 0 \quad \cdots (**)$

これを解くと　$t = \dfrac{bd+1 \pm \sqrt{(bd+1)^2 - 4(b^2d^2 - bd)}}{2}$

$= \dfrac{bd+1 \pm \sqrt{-3(bd-1)^2 + 4}}{2}$

$\sqrt{-3(bd-1)^2+4} \in \mathbb{Z}$ となるのは　$bd = 0, 1, 2$ の時のみ

$bd = 0$ の時　$b = 0$ とすると　③より $ac = -1$　より　$(a, c) = (1, -1), (-1, 1)$

④より $d = \frac{1}{a}$　$\therefore (a, b, c, d) = (1, 0, -1, 1), (-1, 0, 1, -1)$

この時 $a + b\omega = \pm 1$ である。$d = 0$ の時も同様

$bd = 1$ の時　$(**)$ は $t^2 - 2t = 0$ となり　$t = 0, 2$　$\therefore (bc, ad) = (0, 2), (2, 0)$

$bd = 1$ より $b = d = \pm 1$ なので　$(a, b, c, d) = (2, 1, 0, 1), (0, 1, 2, 1)$

$(-2, -1, 0, -1)\ (0, -1, -2, -1)$

いずれの場合も　$a + b\omega = \pm\omega$ 又は $c + d\omega = \pm\omega$

$bd = 2$ の時　$(**)$ は $t^2 - 3t + 2 = 0$　$t = 1, 2$

$(a, b, c, d) = (1, 1, 1, 2)\ (-1, -1, -1, -2), (1, 2, 1, 1), (-1, -2, -1, -1)$

いずれの場合も　$a + b\omega = \pm(1+\omega) = \pm\omega^2$ (複号同順) 又は $c + d\omega = \pm\omega^2$

以上より $\omega - 1$ は素元 (以下 $\omega - 1 = p$ とする) □

2　2.3　補題 2.3.3　$a+b\omega \equiv e+f\omega \pmod{p} \iff a+b \equiv e+f \pmod{3}$

<pr>　$a+b\omega = (\omega-1)(c+d\omega)+e+f\omega$ となる $c+d\omega \in \mathbb{Z}[\omega]$ が存在する

$$
\begin{aligned}
(\text{右辺}) &= -c+(c-d)\omega+d\omega^2+e+f\omega \\
&= -c+(c-d)\omega+d(-1-\omega)+e+f\omega \\
&= e-c-d+(c-2d+f)\omega
\end{aligned}
$$

$$
\therefore \begin{cases} a = e-c-d & \cdots ⑤ \\ b = c-2d+f & \cdots ⑥ \end{cases}
$$

⑤+⑥より $a+b = e+f-3d$ ⋯⑦　∴ $a+b \equiv e+f \pmod{3}$

逆にこの様な e, f に対しては ⑦より d が確定でき、⑤,⑥を満たす c も確定できる。

よって　$a+b\omega \equiv e+f\omega \pmod{p} \iff a+b \equiv e+f \pmod{3}$　□

従って　$a+b\omega \equiv 0, 1, -1 \pmod{p}$ としてよい

補題 2.3.4　$a \equiv \pm 1 \pmod{p}$ の時　$a^3 \equiv \pm 1 \pmod{p^4}$　(複号同順)

<pr>　$a \equiv 1 \pmod{p}$ の時　$a-1 = px$ なる $x \in \mathbb{Z}[\omega]$ が存在し

$$
\begin{aligned}
a^3-1 &\equiv (a-1)(a-\omega)(a-\omega^2) \\
&\equiv px\,(a-1-p)(a-1-p(\omega+1)) \\
&\equiv p^3x\,(x-1)(x-(\omega+1)) \\
&\equiv p^3x\,(x-1)(x+1) \pmod{p^4} \quad (\because -(\omega+1) \equiv 1 \pmod{p})
\end{aligned}
$$

$x \not\equiv x-1$、$x-1 \not\equiv x+1$、$x+1 \not\equiv x$ より $x, x-1, x+1$ のいずれか1つが p の倍数　従って $a^3-1 \equiv 0 \pmod{p^4}$　　$a \equiv -1 \pmod{p}$ の時も同様　□

補題 2.3.5　$\pm 1 \not\equiv \pm\omega$、$\pm\omega \not\equiv \pm\omega^2$、$\pm\omega^2 \not\equiv \pm 1 \pmod{p^2}$　(複号任意)

<pr>　$1 \not\equiv \omega \pmod{p^2}$ のみ示す、その他も全て同様に示せる。

$1 \equiv \omega \pmod{p^2}$ とすると　$p^2 = (\omega-1)^2 = \omega^2-2\omega+1 = -3\omega$ より

$1-\omega = 3\omega(c+d\omega)$ なる $c, d \in \mathbb{Z}$ が存在するが

$$
\begin{aligned}
(\text{右辺}) &= -3c\omega - 3d\omega^2 \\
&= -3c\omega - 3d(-1-\omega) \\
&= 3(d-c) + 3d\omega
\end{aligned}
$$

$$
\begin{cases} 1 = 3(d-c) \\ -1 = 3d \end{cases}
$$

$1 \not\equiv 0 \pmod{3}$、$-1 \not\equiv 0 \pmod{3}$ よりこれを満たす $c, d \in \mathbb{Z}$ は存在せず矛盾。

よって　$1 \not\equiv \omega \pmod{p^2}$　□

2　2.4 証明

$a^3+b^3=ec^3$ (e:単元) を満たす $a,b,c\in\mathbb{Z}[\omega]\setminus\{0\}$ が存在しないことを示す.

<pf> $a^3+b^3=ec^3$ を満たす $a,b,c\in\mathbb{Z}[\omega]\setminus\{0\}$ が存在すると仮定する.

補題 2.4.1　a,b,c のいずれか1つは p の倍数である.

<pf> $a\not\equiv0,\ b\not\equiv0,\ c\not\equiv0 \pmod p$ とすると

$a\equiv\pm1,\ b\equiv\pm1,\ c\equiv\pm1 \pmod p$ (複号任意) であり 補題 2.3.4 より

$a^3+b^3=ec^3$ ∴ $\pm1\pm1\equiv\pm e \pmod{p^4}$

$\pm1\pm1\pm e\equiv0 \pmod{p^4}$ (複号任意)

$p^4=(p^2)^2=9\omega^2=-9-9\omega$ より

$a+b\omega\equiv0 \pmod{p^4}$ である為には $a\equiv b\equiv0 \pmod 9$ が必要だが

補題 2.3.1 より $e=\pm1,\pm\omega,\pm\omega^2$ なので $\pm1\pm1\pm e\not\equiv0 \pmod{p^4}$

よって a,b,c の内いずれか1つは p の倍数である. ∎

補題 2.4.2　$p|c$ としてよい

<pf> $p|a,\ p\nmid c$ の時 $p\nmid b$ が必要で

$a^3+b^3=ec^3$ ∴ $\pm1\equiv\pm e \pmod{p^4}$

∴ $\pm1\equiv\pm e \pmod{p^2}$

∴ $e=\pm1$ (∵ 補題 2.3.5)

この時 $(-b)^3+(\pm c)^3=a^3$　1は単数なので $p|c$ と同様に扱える.

$p|b,\ p\nmid c$ の時も同様 ∎

補題 2.4.3　$(a,b)=(b,c)=(c,a)=1$ としてよい

<pf> $q|a,b$ なる素元 q が存在するとすると, $a^3+b^3=ec^3$ より $q|c^3$

$\mathbb{Z}[\omega]$ は一意分解環なので $q|c$　この時 $\frac{a}{q},\frac{b}{q},\frac{c}{q}\in\mathbb{Z}[\omega]$ であり

$\left(\frac{a}{q}\right)^3+\left(\frac{b}{q}\right)^3=e\left(\frac{c}{q}\right)^3$　これを繰り返すことで $(a,b)=1$ とできる　b,c、c,a も同様 ∎

補題 2.4.4　$\mathrm{ord}_p\, c\geq2$

<pf> $p\nmid a,\ p\nmid b$、$a^3+b^3=ec^3$ より $\pm1\pm1\equiv0 \pmod p$ (複号任意)

∴ $a\equiv\pm1$　$b\equiv\mp1 \pmod p$ (複号同順)

この時 $a^3+b^3=ec^3$ より $\pm1\mp1\equiv ec^3 \pmod{p^4}$ (複号同順)　(∵ 補題 2.3.4)

∴ $c^3\equiv0 \pmod{p^4}$　p は素元なので $\mathrm{ord}_p\, c\geq2$ ∎

以降 $\mathrm{ord}_p\, c=k$ $(k\geq2)$ とする.

NO.

DATE

2　2.4　2の時　$a^3+b^3=ec^3$ より

$$(a+b)(a+b\omega)(a+b\omega^2)=c^3$$

ord_p(右辺) $=3k\geqq 6$ より $a+b$、$a+b\omega$、$a+b\omega^2$ の内少なくとも1つは p^2 の倍数

$p^2\mid a+b$ としてよい（もし $p^2\mid a+b\omega$ であるならば b を $b\omega^2$、$b\omega$ を $b\omega$ を b、$b\omega^2$ を $b\omega$ におきかえて考えればよい。$p^2\mid a+b\omega^2$ であっても同様）

$$(a+b,\ a+b\omega)=((a+b\omega)-(a+b),\ a+b)$$
$$=(pb,\ a+b)$$
$$=p\quad (\because (a,b)=1,\ p\mid a+b)$$

$a+b\omega=(a+b)+pb$、$\mathrm{ord}_p(a+b)\geqq 2$、$\mathrm{ord}_p(pb)=1$ ($\because p\nmid b$) より $\mathrm{ord}_p(a+b\omega)=1$

$a+b\omega=(a+b)+p(\omega+1)b$　　$\omega+1\equiv p+2\not\equiv 0 \pmod p$ より $\mathrm{ord}_p(a+b\omega^2)=1$

従って
$$\begin{cases} a+b=e_1\alpha^3p^{3k-2} & \cdots ⑧\\ a+b\omega=e_2\beta^3p & \cdots ⑨\\ a+b\omega^2=e_3\gamma^3p & \cdots ⑩\end{cases}$$

を満たす単元 e_1、e_2、e_3、$\alpha,\beta,\gamma\in\mathbb{Z}[\omega]$ ($p\nmid\alpha$、$p\nmid\beta$、$p\nmid\gamma$、$(\alpha,\beta)=(\beta,\gamma)=(\gamma,\alpha)=1$)

が存在する。

⑧＋⑨×ω＋⑩×ω^2 より

$$0=e_1\alpha^3p^{3k-2}+\omega e_2\beta^3p+\omega^2e_3\gamma^3p$$
$$-e_1\alpha^3p^{3k-3}=\omega e_2\beta^3+\omega^2e_3\gamma^3$$
$$(-\alpha p^{k-1})^3=\omega e_2e_1^{-1}\beta^3+\omega^2e_3e_1^{-1}\gamma^3\quad\cdots(***)$$

(左辺) $\equiv 0 \pmod{p^2}$ より $\omega e_2e_1^{-1}\beta^3\equiv-\omega^2e_3e_1^{-1}\gamma^3 \pmod{p^2}$

$p\nmid\beta$、$p\nmid\gamma$ より　$\beta^3\equiv\pm1$　$\gamma^3\equiv\pm1 \pmod{p^4}$ （∵補題2.3.4）

$$\therefore \beta^3\equiv\pm1\quad \gamma^3\equiv\pm1 \pmod{p^2}$$
$$\therefore \pm\omega e_2e_1^{-1}\equiv\pm(\omega^2e_3e_1^{-1})\quad (\text{符号任意})$$

従って $\omega e_2e_1^{-1}=e_4$ とすると $\omega^2e_3e_1^{-1}=\pm e_4$

この時 (***) は $(-\alpha p^{k-1})^3=e_4\beta^3\pm e_4\gamma^3$

$$e_4^{-1}(-\alpha p^{k-1})^3=\beta^3+(\pm\gamma)^3$$

以上より $\mathrm{ord}_p c=k_1$ ($k_1\geqq 2$) となる様な $a_1^3+b_1^3=ec_1^3$ を満たす組 (a_1,b_1,c_1) が存在したとすると、$\mathrm{ord}_p c=k_1-1$ となる様な $a_2^3+b_2^3=ec_2^3$ を満たす組 (a_2,b_2,c_2) が存在する。この降下を有限回繰り返すことで $\mathrm{ord}_p c=2$ となる様な解の組の存在が言え、最終的に $\mathrm{ord}_p c=1$ の時の解の組の存在を認めることになるが、補題2.4.4 より $\mathrm{ord}_p c=1$ となることはない。

従って $a^3+b^3=ec^3$ を満たす解の組 $a,b,c\in\mathbb{Z}[\omega]\setminus\{0\}$ は存在しない ▭

1は単元であり、$\mathbb{Z}\subset\mathbb{Z}[\omega]$ なので $n=3$ の時のフェルマーの最終定理は成り立つ。

NO.

DATE

3 参考文献

雪江明彦著『整数論1 初等整数論からp進法へ』（日本評論社） 6.1、6.3、6.6、8.4、8.7.

4 終わりに

今回が初めての記事となります。最初は「フェルマーの最終定理のn=3,4位なら高校数学の範囲で示せるのでは?」などと高をくくり、自分一人で示してみたのですが、細かなミスや議論の不備だけでなく、大きな計算ミスまで発覚してしまい、n=3の方は一から練り直すことになりました。これらのことを指摘して下さり、その後も自分の変な証明を辛抱強く校正して下さり、そして困った時にはヒントを与え、本まで貸して下さった前部長のN山さんには感謝してもしつくせません。本当にありがとうございました。そして、ここまで字の汚ない自分の文章(?)に付き合って下さった皆様、ありがとうございました。どうぞ他の人のクオリティの高い記事にも目を通して下さい。

累乗和の考察

高校2年2組34番上村俊貴

§1. はじめに

本日は第70回灘校文化祭、および数学研究部にお越し頂き、誠にありがとうございます。当初カーティスの定理の拡張について載せる予定でしたが、予定変更となり、累乗和について載せることになりました。
このテーマについては高校数学の知識があれば大体読めるような記事となっております。

§2. 累乗和について

高校数学の教科書では3乗和の公式までが載っていますが、4乗以降は載っていません。今回はそれらを導出する式を作ることにします。

2-1. 普通の方法での4乗和の証明

nを正の整数として、

$$\sum_{k=1}^{n}\left\{(k+1)^5-k^5\right\}=(n+1)^5-1$$

について考えると、次のように変形できる。

$$5\sum_{k=1}^{n}k^4+10\sum_{k=1}^{n}k^3+10\sum_{k=1}^{n}k^2+5\sum_{k=1}^{n}k+n$$

$$=(n+1)^5-1$$

3乗和までの公式を利用して計算すると、

$$\sum_{k=1}^{n}k^4=\frac{1}{5}n^5+\frac{1}{2}n^4+\frac{1}{3}n^3-\frac{1}{30}n$$

が得られる。この方法が一般的かもしれないが、5乗以降から計算が煩雑となり厳しい。そこで上のような方法を少しだけアレンジする。

2-2. 微積分を用いた拡張

def. $\sum_{k=0}^{n}k^m=S_m(n)$ と表記する。

ここで次の等式が任意の $n\in\mathbb{Z}^+$ で成立する。

$$S_{m+1}(n)-S_{m+1}(n-1)=n^{m+1} \quad ①$$

n を実数 x まで拡張し、多項式 $S_m(x)$ を考えると、

$$S_{m+1}(x)-S_{m+1}(x-1)=x^{m+1} \quad ②$$

は①より無限個の正の整数値を代入しても成立しており、左辺が x に関する $m+2$ 次多項式であることに注意すれば②は多項式として等しい。多項式は微分可能なので②の両辺を x で微分し、

$$S'_{m+1}(x)-S'_{m+1}(x-1)=(m+1)x^m$$

したがって，xに1からnまでの正の整数値を代入することを考え辺々足すと，

$$\sum_{x=1}^{n}\left(S'_{m+1}(x)-S'_{m+1}(x-1)\right)=(m+1)\sum_{x=1}^{n}x^{m}$$

ゆえに，$S'_{m+1}(n)-S'_{m+1}(0)=(m+1)S_m(n)$

$\iff S'_{m+1}(n)=(m+1)S_m(n)+S'_{m+1}(0)$ —③

nを実数xまで拡張した次の多項式

$$S'_{m+1}(x)=(m+1)S_m(x)+S'_{m+1}(0) \quad —④$$

は③より任意の正の整数値で成立するので，両辺がxに関する$m+1$次多項式であることに注意して，④は多項式として等しい。

多項式は積分可能なので，④の両辺を0〜nまでxで積分して，

$$\int_0^n S'_{m+1}(x)dx=\int_0^n(m+1)S_m(x)dx+\int_0^n S'_{m+1}(0)dx$$

$$\therefore S_{m+1}(n)-S_{m+1}(0)=(m+1)\int_0^n S_m(x)dx+nS'_{m+1}(0)$$

$S_{m+1}(0)=0$なので，$S'_{m+1}(0)=B_{m+1}$とすると，

$$S_{m+1}(n)=(m+1)\int_0^n S_m(x)dx+nB_{m+1} \quad —⑤$$

と書ける。したがって，$S_4(n)$について，⑤より，

$$S_4(n) = 4\int_0^n S_3(x)\,dx + nB_4$$
$$= 4\int_0^n \frac{x^2(x+1)^2}{4}\,dx + nB_4$$
$$= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + nB_4$$

$S_4(1) = 1$ より, $1 = \frac{1}{5} + \frac{1}{2} + \frac{1}{3} + B_4$

$$\therefore B_4 = -\frac{1}{30}$$

ゆえに $S_4(n) = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$

同様にして, $S_5(n) = \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2$

$$S_6(n) = \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 - \frac{1}{6}n^3 + \frac{1}{42}n$$

などが順番に示される。これにより、先で行った普通の方法よりも大幅に計算量は軽減されるものの、やはりそれなりに大変になってしまう。
なお上の式中に出てきた B_m はベルヌーイ数と呼ばれ, $B_5 = 0$, $B_6 = \frac{1}{42}$ は上の手順から導かれる。

§3、おわりに

今回扱ったテーマは割と理解しやすいものだったと思います。ただ、どうしても分かりにくい表現が途中にあると思うので、そこはご了承いただければ幸いです。

幾何学の考察

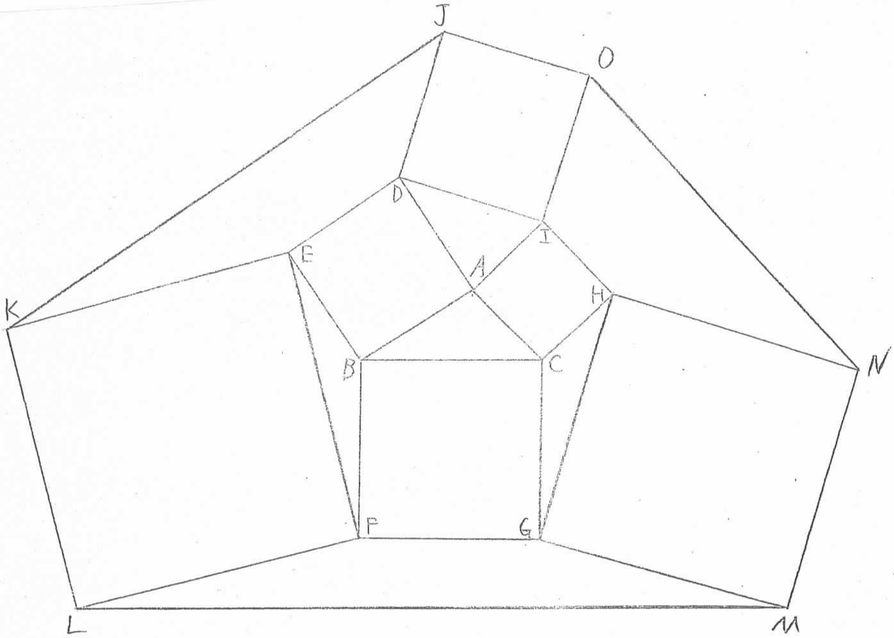
高校2年2組34番 上村俊貴

§1. はじめに

本日は第70回灘校文化祭、および数学研究部にお越し頂き、誠にありがとうございます。当初カーティスの定理の拡張について載せる予定でしたが、予定変更となり、幾何学の考察を載せることになりました。このテーマについては、幅広い年齢層の方々を対象としており、小学生の方々にも内容理解がしやすいものとなっておりますので、簡単に思うかもしれませんが予めご了承下さい。

§2. 幾何学の考察

今回扱う図形は下図である。
なお中央部に見える図形は誰もが見たことのある図形だが、これを拡張した図形について考えていく。



上図において、△ABCは任意の三角形で、四角形ADEB・四角形BFGC・四角形ACHI・四角形DIOJ・四角形EKLF・四角形HGMNは全て正方形である。

以下では四角形JKED，四角形OIHN，
四角形FLMGの面積について考える。

$\overrightarrow{AB}=\begin{pmatrix}a\\b\end{pmatrix}$, $\overrightarrow{AC}=\begin{pmatrix}c\\d\end{pmatrix}$ とすると，

$\overrightarrow{AD}=\begin{pmatrix}b\\-a\end{pmatrix}$, $\overrightarrow{AI}=\begin{pmatrix}-d\\c\end{pmatrix}$, $\overrightarrow{DI}=\begin{pmatrix}-d-b\\c+a\end{pmatrix}$

$\overrightarrow{DJ}=\begin{pmatrix}-c-a\\-d-b\end{pmatrix}$, $\overrightarrow{DE}=\begin{pmatrix}a\\b\end{pmatrix}$

$\triangle DEJ=\frac{1}{2}\left|-ad-ba+bc+ab\right|=\frac{1}{2}\left|ad-bc\right|$

$\overrightarrow{BC}=\begin{pmatrix}c-a\\d-b\end{pmatrix}$, $\overrightarrow{BF}=\begin{pmatrix}d-b\\a-c\end{pmatrix}$, $\overrightarrow{BE}=\begin{pmatrix}b\\-a\end{pmatrix}$,

$\overrightarrow{EF}=\begin{pmatrix}d-2b\\2a-c\end{pmatrix}$, $\overrightarrow{EK}=\begin{pmatrix}2a-c\\2b-d\end{pmatrix}$,

$\overrightarrow{EJ}=\begin{pmatrix}-2a-c\\-2b-d\end{pmatrix}$, $\triangle EKJ=\frac{1}{2}\left|(-2a-c)(2b-d)-(2a-c)(-2b-d)\right|$

$=2\left|ad-bc\right|$

$\therefore$ (四角形JKED)

$=\triangle DEJ+\triangle EKJ=\frac{5}{2}\left|ad-bc\right|$

$=5\triangle ABC$

$$\overrightarrow{IO}=\begin{pmatrix}-c-a\\-b-d\end{pmatrix},\ \overrightarrow{IH}=\begin{pmatrix}c\\d\end{pmatrix}$$

$$\therefore \triangle OIH=\frac{1}{2}\left|(-c-a)d-c(-b-d)\right|=\frac{1}{2}|ad-bc|$$

$$\overrightarrow{CG}=\begin{pmatrix}-b+d\\a-c\end{pmatrix},\ \overrightarrow{CH}=\begin{pmatrix}-d\\c\end{pmatrix},\ \overrightarrow{GH}=\begin{pmatrix}-2d+b\\2c-a\end{pmatrix}$$

$$\overrightarrow{HN}=\begin{pmatrix}2c-a\\2d-b\end{pmatrix},\ \overrightarrow{HO}=\begin{pmatrix}-2c-a\\-b-2d\end{pmatrix}$$

$$\therefore \triangle OHN=\frac{1}{2}\left|(2c-a)(-b-2d)-(-2c-a)(2d-b)\right|$$

$$=2|ad-bc|$$

$\therefore$ (四角形 OIHN)

$$=\triangle OIH+\triangle OHN=\frac{5}{2}|ad-bc|$$

$$=5\triangle ABC$$

$$\overrightarrow{FL}=\begin{pmatrix}2a-c\\2b-d\end{pmatrix},\ \overrightarrow{FG}=\begin{pmatrix}c-a\\d-b\end{pmatrix}$$

$$\therefore \triangle FLG=\frac{1}{2}\left|(2a-c)(d-b)-(c-a)(2b-d)\right|$$

$$=\frac{1}{2}|ad-bc|$$

$\overrightarrow{GM} = \begin{pmatrix} 2c-a \\ 2d-b \end{pmatrix}$, $\overrightarrow{GL} = \begin{pmatrix} 3a-2c \\ 3b-2d \end{pmatrix}$

$$\therefore \triangle GLM = \frac{1}{2}\left|(2c-a)(3b-2d) - (3a-2c)(2d-b)\right|$$
$$= 2|ad-bc|$$

$\therefore$ (四角形FLMG)

$= \triangle FLG + \triangle GLM = \frac{5}{2}|ad-bc|$

$= 5\triangle ABC$

したがって,

(四角形JKED)＝(四角形OIHN)＝(四角形FLMG)
$= 5\triangle ABC$

であることが示された。

また, $|\overrightarrow{JK}| = |\overrightarrow{EK} - \overrightarrow{EJ}| = \left|\begin{pmatrix} 4a \\ 4b \end{pmatrix}\right| = 4|\overrightarrow{AB}|$

$|\overrightarrow{ON}| = |\overrightarrow{HN} - \overrightarrow{HO}| = \left|\begin{pmatrix} 4c \\ 4d \end{pmatrix}\right| = 4|\overrightarrow{AC}|$

$$\left|\overrightarrow{LM}\right| = \left|\overrightarrow{GM} - \overrightarrow{GL}\right| = \left|\begin{pmatrix} 4c-4a \\ 4d-4b \end{pmatrix}\right| = 4\left|\overrightarrow{BC}\right|$$

であるから，$JK = 4AB$

$ON = 4AC$

$LM = 4BC$ と分かる。

以上のことから，

四角形JKEDをDEがABに重なるように，

四角形ONHIをIHがACに重なるように，

四角形FLMGをFGがBCに重なるように

平行移動させることで，△ABCを4倍に

相似拡大させた三角形が作れることが分かります。

§3、おわりに

今回扱ったテーマは幅広い年齢層の方々に少しでも楽しめるような，そして理解しやすいようなものだったと思います。ここまで読んで下さりありがとうございました。来年はもっとレベルの高い記事を書きたいと思います。

切断点を k 個もつ連結グラフの数え上げ

高校 2 年 4 組 26 番　田嶋 璃久

1　はじめに

本日は灘校文化祭、および数学研究部にお越し頂き誠にありがとうございます。この記事は切断点を k 個もつ連結グラフの数え上げをしたものです。本当はハミルトングラフというグラフの数え上げをしようと思っていましたが、実力が足りずできなかったのでこれにしました。自分は新高なので部誌を書くのが初めてですが、読んでいただければ幸いです。

2　準備

ここでは、この後使用する用語の定義をし、必要な定理を紹介します。

定義 1（通常型母関数） 数列 $\{a_n\}$ の第 n 項 a_n を x^n の係数とする形式的べき級数

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

を数列 a_n の通常型母関数という。

定義 2（指数型母関数） 数列 $\{a_n\}$ の第 n 項 a_n を $\frac{x^n}{n!}$ の係数とする形式的べき級数

$$F(x) = a_0 + a_1 \tfrac{x}{1!} + a_2 \tfrac{x^2}{2!} + \cdots + a_n \tfrac{x^n}{n!} + \cdots$$

を数列 $\{a_n\}$ の指数型母関数という。

この母関数では、加法や乗法は通常の級数と同様に定義され、結合律や交換律などの代数のよく知られた法則が成り立ちます。また、母関数の形式導関数も同様に定義されます。母関数を使うことで有限集合の元の個数を数えやすくなるので、この記事でも母関数を使って数え上げようと思います。次の定理は数え上げで有効な道具となる定理です。

定理 3 $A(x) = \displaystyle\sum_{m=0}^{\infty} a_m x^m, F(x) = \sum_{m=1}^{\infty} b_m x^m$ に対し、$A(x) = e^{F(x)}$ を満たすとする。このとき、$m \geqq 1$ に対し、

$$b_m = a_m - \frac{1}{m}\left(\sum_{k=1}^{m-1} k b_k a_{m-k}\right)$$

が成り立つ。（証明省略）

定理 4　$A(x)=\sum_{m=0}^{\infty}a_m x^m, F(x)=\sum_{m=1}^{\infty}b_m x^m$ に対し、$A(x)=e^{F(xA(x))}$ が成り立つとする。このとき、正整数 k に対し、$(xA(x))^k=\sum_{m=k}^{\infty}H(m,k)x^m$ と書くと、

$$b_m=H(m+1,1)-\frac{m+1}{m}\sum_{l=1}^{m-1}\frac{lb_l}{l+1}H(m+1,l+1)$$

が成り立つ。（証明省略）

次に、グラフ理論の用語を説明します。

定義 5（標識単純グラフ）　空でない有限集合 V をとり、V の元の対の集合 $\binom{V}{2}=\{\{i,j\}\subset V|i\neq j\}$ を定め、写像 $gv:\binom{V}{2}\to\{0,1\}$ を（V 上）標識単純グラフという。

これからは、これを標識グラフと呼ぶことにします。

定義 6（点、辺、位数、大きさ）　標識グラフ gv について、V の元を点と呼び、含まれる点の個数を gv の位数という。また、各 $\{i,j\}\in\binom{V}{2}$ に対し、 $g(\{i,j\})=1$ のとき、$\{i,j\}$ を gv の辺といい、gv の辺の数を gv の大きさという。

例があった方が分かりやすいので、例を出します。

例　$V=\{1,2,3,4\}$ に対し、写像 $gv:\binom{V}{2}\to\{0,1\}$ を、$gv(\{1,2\})=1, gv(\{1,3\})=0, gv(\{1,4\})=0, gv(\{2,3\})=1, gv(\{2,4\})=0, gv(\{3,4\})=1$ により定める。このとき、標識グラフ gv の位数は 4 であり、大きさは 3 である。また、gv の辺は、$\{1,2\},\{2,3\},\{3,4\}$ である。(図 1)

定義 7（根、根つき標識グラフ、（非標識根つき）標識グラフ）　標識グラフ gv の点 v を他の点と区別する特定の点と考えたとき、v を gv の根といい、その gv を根つき標識グラフという。また、根には標識をつけないが、他の点に標識づけた場合の根つき標識グラフを（非標識根つき）標識グラフという。

定理 8　ある性質 P をもつ位数 n の標識グラフの個数を $\frac{x^n}{n!}$ の係数にもつ指数型母関数を $F(x)$ とし、性質 P をもつ位数 n の根つき標識グラフの個数を $\frac{x^n}{n!}$ の係数にもつ指数型母関数を $F^{(r)}(x)$ とする。このとき、

$$F^{(r)}(x)=x\tfrac{dF(x)}{dx}$$

である。また、性質 P をもつ位数 n の（非標識根つき）標識グラフの個数を $\frac{x^n}{n!}$ の係数にもつ指数型母関数は

$$\tfrac{F^{(r)}(x)}{x}=\tfrac{dF(x)}{dx}$$

である。

証明　性質 P をもつ標識グラフの数え上げ母関数 $F(x)$ を

$$F(x)=\sum_{n=1}^{\infty}a_n\frac{x^n}{n!}$$

とおく。位数 n の標識グラフ 1 つからは根つき標識グラフが n 通り生まれる。これはおのおのの点が根の候補になり得るからである。よって、

$$F^{(r)}(x) = \sum_{n=1}^{\infty} n a_n \frac{x^n}{n!} = x \sum_{n=1}^{\infty} a_n \frac{x^{n-1}}{(n-1)!} = x \frac{dF(x)}{dx}$$

である。また、

$$\tfrac{F^{(r)}(x)}{x} = \tfrac{dF(x)}{dx}$$

の定数項は根に対応し、$n \geqq 1$ に対し $\frac{x^n}{n!}$ の係数は位数 $n+1$ の（非標識根つき）標識グラフの個数を表す。■

（非標識根つき）標識グラフに対する指数型母関数に x をかけることで標識づけられていない根を標識づけることを意味するということがこの定理において重要なことである。

例　標識グラフの数え上げ母関数を

$$G(x) = \sum_{n=1}^{\infty} 2^{\binom{n}{2}} \frac{x^n}{n!}$$

とおく。（位数 n の標識グラフは $2^{\binom{n}{2}}$ 個である。）位数 n の根つき標識グラフの個数である $n2^{\binom{n}{2}}$ を $\frac{x^n}{n!}$ の係数とする根つき標識グラフの数え上げ指数型母関数を $G^{(r)}(x)$ とすると、

$$G^{(r)}(x) = x \tfrac{dG(x)}{dx}$$

が成り立っていることがわかる。また、（非標識根つき）標識グラフの数え上げ指数型母関数は

$$\tfrac{G^{(r)}(x)}{x} = \tfrac{dG^(x)}{dx}$$

となっている。

定理 9　性質 P をもつ位数 k の標識グラフの個数を a_k とし、指数型母関数

$$a(x) = \sum_{k=1}^{\infty} a_k \frac{x^k}{k!}$$

を考える。このとき、$a^s(x)$ における $\frac{x^n}{n!}$ の係数は性質 P をもつ互いに共通の点をもたない s 個のグラフからなる組 $(g_1, g_2, \cdots, g_s)$ の個数である。そこで、n は s 個のグラフの位数の和である。（証明略）

注意 10　定理 9 で述べた s 個のグラフの組の要素の順序を考慮に入れない場合は $a^s(x)$ を $s!$ で割る必要がある。また、ある指数型母関数 $F(x)$ で $\displaystyle\sum_{s=1}^{\infty} \frac{a^s(x)}{s!}$ が表される、つまり

$$F(x) = \sum_{s=1}^{\infty} \frac{a^s(x)}{s!}$$

とすると、

$$1 + F(x) = e^{a(x)}$$

が成り立つ。

3　連結グラフ、標識ブロックの数え上げ

定義 11（道、連結）　標識グラフ g における異なった点の列 $v_1, v_2, \cdots, v_k$ が各 $i = 1, 2, \cdots, k-1$ に対し、条件 $\{v_i, v_{i+1}\} \subset E(g)$ を満たすとき、この点列は g の道とよばれる。標識グラフ g のどの 2 点間にも道が存在するとき、g は連結であるという。自明なグラフ（位数 1 の標識グラフ）は連結と定める。

定理 12　$G(x) = 2^{\binom{n}{2}} \frac{x^n}{n!}$ を標識グラフの指数型母関数とし、

$$C(x) = \sum_{n=1}^{\infty} C_n \frac{x^n}{n!}$$

を連結な標識グラフに対する指数型母関数とする。ここで、C_n は位数 n の連結な標識グラフの個数である。このとき、定理 9, 注意 10 より、

$$1 + G(x) = e^{C(x)}$$

が成り立つ。また、定理 3 を使うと、

$$C_n = 2^{\binom{n}{2}} - \frac{1}{n} \sum_{k=1}^{n-1} k \binom{n}{k} 2^{\binom{n-k}{2}} C_k$$

が得られる。これを利用して $C(x)$ の初めのいくつかの項を求めると、

$$C(x) = x + \tfrac{x^2}{2!} + 4\tfrac{x^3}{3!} + 38\tfrac{x^4}{4!} + 728\tfrac{x^5}{5!} + \cdots$$

となる。

定義 13（切断点、標識ブロック）　標識グラフ g の点 v について、$g - v$ が非連結であるならば、v を g の切断点という。切断点をもたない標識グラフを標識ブロックという。

定理 14　位数 n の標識ブロックの個数を B_n とし、指数型母関数

$$B(x) = \sum_{n=1}^{\infty} B_n \frac{x^n}{n!}$$

を考える。グラフ理論の本では自明な標識グラフは標識ブロックと定めているが、ここでは $B_1 = 0$ とする。このとき、

$$C'(x) = \exp\{B'(xC'(x))\}$$

が成り立つ。

証明　定理 8 を使い、連結な根つき標識グラフに対する指数型母関数

$$C^{(r)}(x) = x\tfrac{dC(x)}{dx}$$

を考える。連結な根つき標識グラフのうち、根にただ 1 つのブロックが付随している場合の指数型母関数を $C_1^{(r)}(x)$ とおく。最初に $C^{(r)}(x)$ と $C_1^{(r)}(x)$ との関係式を導き、その後に $C_1^{(r)}(x)$ と $B(x)$ との関係式を導くことにより定理の証明が完了する。まずは、$C^{(r)}(x)$ と $C_1^{(r)}(x)$ の関係式を導く。根にただ 1 つのブロックが

付随している連結な（非標識根つき）標識グラフに対する指数型母関数は定理 8 より、

$$\frac{C_1^{(r)}(x)}{x}$$

である。これらの標識グラフのうち、s 個のそれを要素にする組に対する指数型母関数は定理 9 より、

$$\left(\frac{C_1^{(r)}(x)}{x}\right)^s$$

である。組の要素の順序を考えないとすると、注意 10 より対象とする指数型母関数は、

$$\frac{\left(\frac{C_1^{(r)}(x)}{x}\right)^s}{s!}$$

である。ここで組を構成している s 個の要素のおのおのの根をまとめて合体させ 1 つの点とみなす (図 2)。その点を新たに根とする（非標識根つき）標識グラフを生成すると、この根にちょうど s 個のブロックが付随したものになる。このような考察は等式

$$\frac{C^{(r)}(x)}{x} = 1 + \sum_{s=1}^{\infty} \frac{\left(\frac{C_1^{(r)}(x)}{x}\right)^s}{s!}$$

を生み出し、したがって等式

$$\frac{C^{(r)}(x)}{x} = \exp\left(\frac{C_1^{(r)}(x)}{x}\right)$$

が得られる。

次に $C_1^{(r)}(x)$ と $B(x)$ との関係式を導く。$a_{k,p}$ を $\left(\frac{C^{(r)}(x)}{x}\right)^{k-1}$ における $\frac{x^p}{p!}$ の係数とする。すなわち、

$$\left(\frac{C^{(r)}(x)}{x}\right)^{k-1} = \sum_{p=1}^{\infty} a_{k,p} \frac{x^p}{p!}$$

$a_{k,p}$ は $k-1$ 個の連結な（非標識根つき）標識グラフを組にしたもので、そのうち標識づけられている点が p 個であるものの個数である。（標識づけられている点は 1 から p までの標識で標識づけられていて、非標識な点（根）は $k-1$ 個あるから、点としては全体として $p+k-1$ 個ある。）これらの組のおのおのに 1 つの点そ加え、この付加した点とはじめの $k-1$ 個の根を点集合にもつ新しい位数 k のブロックを構成する付加した点を根にする位数 $p+k$ の連結な根つき標識グラフは根にただ 1 つのブロックをもち、$C_1^{(r)}(x)$ に寄与する (図 3)。これを 1 から $p+k$ までの標識で標識替えして、そのうち k 個を根に付随したブロックの点に割り当てる。この取り出し方は $\binom{p+k}{k}$ 通りある。取り出した k 個の標識から根を標識する仕方は k 通りである。よって、$kB_k\binom{p+k}{k}$ 個の連結な根つき標識グラフが生まれる。したがって、等式

$$C_1^{(r)}(x) = \sum_{k=1}^{\infty}\sum_{p=1}^{\infty} kB_k \binom{p+k}{k} \frac{x^{p+k}}{(p+k)!} = \sum_{k=1}^{\infty} B_k \frac{x^k}{(k-1)!} \sum_{p=1}^{\infty} a_{k,p} \frac{x^p}{p!}$$

が得られる。

$$\left(\frac{C^{(r)}(x)}{x}\right)^{k-1} = \sum_{p=1}^{\infty} a_{k,p} \frac{x^p}{p!}$$

であるから、

$$C_1^{(r)}(x) = x\sum_{k=1}^{\infty} B_k \frac{\left(C_1^{(r)}(x)\right)^{k-1}}{(k-1)!}$$

と書き直される。したがって、

$$\tfrac{C_1^{(r)}(x)}{x} = B'\left(C^{(r)}(x)\right)$$

となる。$C^{(r)}(x) = xC'(x)$ だから、

$$\tfrac{C_1^{(r)}(x)}{x} = B'\left(xC'(x)\right)$$

を得る。$C'(x) = \frac{C^{(r)}(x)}{x} = \exp\left(\frac{C_1^{(r)}(x)}{x}\right)$ だから、

$$C'(x) = \exp\{B'(xC'(x))\}$$

が成り立つ。■

定理 4 を定理 14 に適用すると、次の定理が得られる。

定理 15　$m \geqq 2$ に対し、

$$B_m = (m-1)!H(m,1) - (m-2)!m\sum_{l=1}^{m-2} \frac{lB_{l+1}}{(l+1)!} H(m,l+1)$$

である。

これに基づいて $B(x)$ のはじめのいくつかの項を求めると、

$$B(x) = \tfrac{x^2}{2!} + \tfrac{x^3}{3!} + 10\tfrac{x^4}{4!} + 238\tfrac{x^5}{5!} + 11368\tfrac{x^6}{6!} + \cdots$$

となる。

4　切断点を k 個もつ連結グラフの数え上げ

定理 16　切断点を k 個もつ連結グラフの数え上げ指数型母関数を $J_k(x)$ とする。

$$S_i(x) = \begin{cases} \displaystyle\sum_{s=1}^{\infty} \frac{B'(x)^s}{s!} = e^{B'(x)} (i=1) \\ \displaystyle\sum_{s=0}^{\infty} B^{(i)}(x)^s (i \geqq 2) \end{cases} ,R_{k,l}(x) = \prod_{i=l}^{k} S_i(x)^{\binom{k}{i}}$$

としたとき、

$$J_k^{(k)}(x) = \frac{1}{k!}\left(R_{k,1}(x) - \sum_{i=1}^{[\frac{k}{2}]} R_{i,1}(x)R_{k-i,1}(x)\right)$$

が成り立つ。

定理 8, 定理 9, 注意 10 より、$S_1(x)$ は（非標識根つき）標識ブロック s 個の組の数え上げ指数型母関数を $s=0$ から足し合わせているものだとわかる。同様に、$i \geqq 2$ の $S_i(x)$ でも形式的に非標識な根を i 個とって、

その i 個の根を含むような（非標識根つき）標識ブロックの個数を考えている。ここで、標識ブロックを数え上げたとき（前半）のように、s 個の非標識な根を 1 つに重ねると、$S_i(x)$ は i 個の非標識な根を含む s 個の標識ブロックがついているようなグラフの数え上げ指数型母関数を $s=0$ から足し合わせているとわかる。このグラフの根にはブロックでないグラフは付随していない。つまり、根以外の点が切断点になることがないのである。これを利用する。

証明　まず、k 個の形式的な非標識な点（根）をとる。この k 個の根が切断点になるようなグラフを数え上げる。図 4 では $k=3$ で考えているが、指数型母関数 $S_i(x)$ を呼び起こす原因となるブロックの組が $\binom{k}{i}$ 個ある。だが、実際に切断点を k 個もたない場合 (図 5) はある根においてその 1 つの根だけを含むブロックが存在しない場合、つまり $s=0$ の場合である。任意の根において $s>0$ である必要があるから、$s=0$ を除いて、($S_1(x)$ のみ $s=0$ を除いているのはこのため。) 母関数は

$$\frac{1}{k!}R_{k,1}(x)$$

となる。連結でない場合は、根がつながっていないから、つながっていない根を分けて、分け方で分類する。ただし、今考えている母関数では根にブロックがついていない場合 ($s=0$) も含むから、わけた根が必ずしもすべてつながっている必要がないとする。例えば、$k=5$ のときは、$(4,1),(3,2),(3,1,1),(2,2,1),(2,1,1,1),(1,1,1,1,1)$ と分類できるが、$(3,1,1)$ は $(4,1)$ の特別な場合 (分けたときに 4 つの根が含まれる方で 1 つの根だけがつながっていない場合) として見なせるので、実質的には $(4,1),(3,2)$ の 2 通りの分類しかない。同様に、一般的な k でも $(k-1,1),(k-2,2),\cdots,(k-[\frac{k}{2}],[\frac{k}{2}])$ というように分類できる。$(k-i,i)$ という分類のとき $S_j(x)$ を呼び起こすブロックの組は $\binom{i}{j}+\binom{k-i}{j}$ 個であるから、

$$J_k^{(k)}(x)=\frac{1}{k!}R_{k,1}(x)-\frac{1}{k!}\sum_{i=1}^{[\frac{k}{2}]}\prod_{j=1}^{i}S_j(x)^{\binom{i}{j}+\binom{k-i}{j}}=\frac{1}{k!}\left(R_{k,1}(x)-\sum_{i=1}^{[\frac{k}{2}]}R_{i,1}(x)R_{k-i,1}(x)\right)$$

を得る。($J_k(x)$ を k 階微分したのは非標識な根が k 個あるから。)■

5　おわりに

時間と実力が不足しているせいで $J_k(x)$ における $\frac{x^n}{n!}$ の具体的な係数をもとめることができずに終わってしまったのは残念でした。でも、昨年度のゼミで学んだことを部誌の記事という形で残すことができたことに関してはとてもうれしく思います。$J_k(x)$ と $B(x)$ の関係式をもとめるのには苦労しましたが、最終的に自分で納得がいく答えにたどり着けたので良かったです。

＜参考文献＞グラフの数え上げ　-母関数を礎にして- 田澤　新成著

次のページに図をのせておきます。(パソコンでかく能力がないため。)

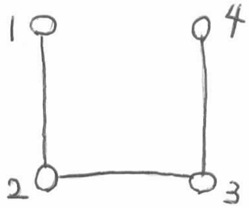


図1

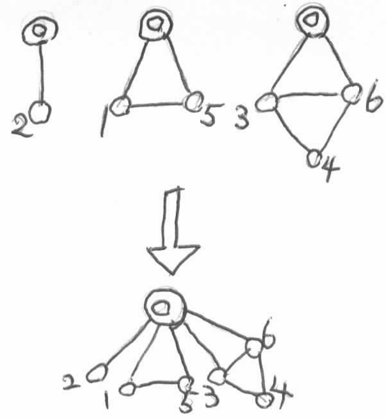


図2　(非標識根つき)標識グラフの合体

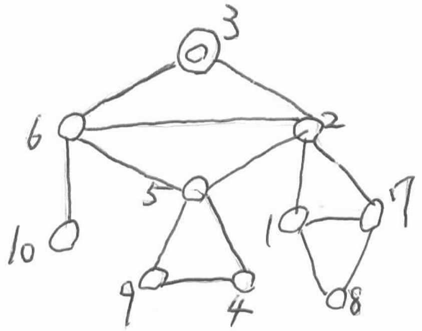


図3　根にただ1つのブロックをもつ標識グラフ

図4　$S_1(x)$に寄与する部分　　$S_2(x)$に寄与する部分　　$S_3(x)$に寄与する部分

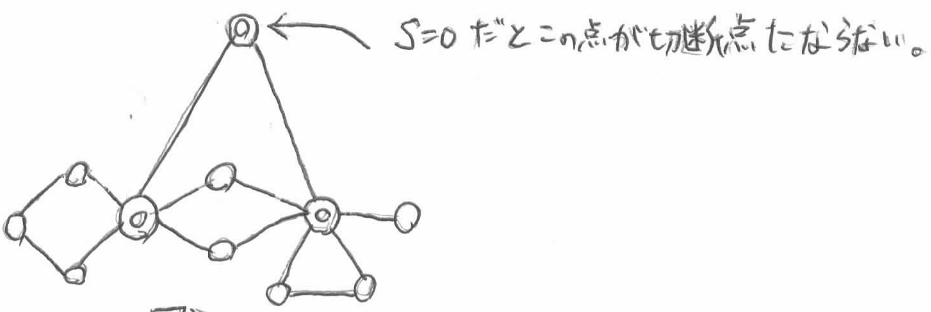


図5

チェビシェフ多項式の係数

高校 3 年 2 組 35 番　中山裕大

1　はじめに

本日は灘校文化祭及び数学研究部にお越しいただき誠にありがとうございます. この記事では, チェビシェフ多項式の係数を求めます. 是非お読みください.

2　準備

以下必要な知識を証明抜きに書く.

$a := b$ とは a を b(に等しいもの) として定義するということを意味する.$\mathbb{Z}^+, \mathbb{N}_0, \mathbb{Z}, \mathbb{C}$ はそれぞれ正の整数, 非負整数, 整数, 複素数の集合とする.$c \in \mathbb{C}$ に対し,$c\mathbb{Z} := \{cn \in \mathbb{C} | n \in \mathbb{Z}\}$ とする. 実数 c の小数部分を $\{c\}$ で表す.$n \in \mathbb{N}_0$, 数列 $\{a_i\}_{i=1}^{\infty}$ に対し

$$\prod_{k=1}^{n} a_k := \begin{cases} a_1 a_2 \dots a_n & (n > 0) \\ 0 & (n = 0) \end{cases}$$

等とする.

以下,$z \in \mathbb{C}$ に対し

$$e^z := \sum_{n=0}^{\infty} \frac{z^n}{n!}$$
$$\cos z := \frac{e^{iz} + e^{-iz}}{2}$$
$$\sin z := \frac{e^{iz} - e^{-iz}}{2i}$$

とする. テイラー展開により, これは実数の上での指数関数や三角関数を複素平面全体に解析接続したものだと分かる. すると, 関数関係不変の原理により, 実数の上での指数関数の基本的性質や三角関数の加法定理, 積和・和積公式等は複素数の上でも成り立つと分かる.

補題 1 $z, w \in \mathbb{C}$ に対し

$\cos z = \cos w \iff (z+w \in 2\pi\mathbb{Z} \vee z-w \in 2\pi\mathbb{Z})$

証明. $\cos z = \cos w$

$\iff \dfrac{e^{iz}+e^{-iz}}{2} = \dfrac{e^{iw}+e^{-iw}}{2}$

$\iff e^{iz}+e^{-iz} = e^{iw}+e^{-iw}$

$\iff e^{iz} = e^{\pm iw}$

(∵(⇒) e^{iz}, e^{-iz}; e^{iw}, e^{-iw} は和が一定で、積も共に1で一定)

$\iff e^{-\mathrm{Im}z + i\mathrm{Re}z} = e^{\mp \mathrm{Im}w \pm i\mathrm{Re}w}$

$\iff e^{-\mathrm{Im}z} e^{i\mathrm{Re}z} = e^{\mp \mathrm{Im}w} e^{\pm i\mathrm{Re}w}$

$\iff e^{-\mathrm{Im}z}(\cos \mathrm{Re}z + i\sin \mathrm{Re}z) = e^{\mp \mathrm{Im}w}(\cos \mathrm{Re}w \pm i\sin \mathrm{Re}w)$

$\iff (e^{-\mathrm{Im}z} = e^{\mp \mathrm{Im}w} \wedge \mathrm{Re}z - \mathrm{Re}(\pm w) \in 2\pi\mathbb{Z})$

(∵(⇒) 両辺の絶対値、偏角をとればよい。)

$\iff (\mathrm{Im}z = \mathrm{Im}(\pm w) \wedge \mathrm{Re}z - \mathrm{Re}(\pm w) \in 2\pi\mathbb{Z})$

$\iff (z-w \in 2\pi\mathbb{Z} \vee z+w \in 2\pi\mathbb{Z})$

(以上全て複号同順) ■

3. チェビシェフ多項式の定義

定理2. $n \in \mathbb{N}_0$ に対し、$\forall z \in \mathbb{C}$, $T_n(\cos z) = \cos(nz)$ なる $\exists$ 整係数多項式 T_n が一意に存在する。

証明. (存在)

n に関する帰納法により示す。$n = 0, 1$ のとき、それぞれ $T_n(z) = 1$, $T_n(z) = z$ とすればよい。

$n = m, m+1$ $(m \in \mathbb{N}_0)$ のとき、条件を満たす T_n が存在するならば、$n = m+2$ のとき、

$\cos((m+2)z) = \cos((m+2)z) + \cos(mz) - \cos(mz)$

$= 2\cos((m+1)z)\cos z - \cos(mz)$

$= 2\cos z\, T_{m+1}(\cos z) - T_m(\cos z)$

より、$T_{m+2}(z) = 2z\, T_{m+1}(z) - T_m(z)$ とすればよい。

よって示された。

(一意性)

T_n, t_n が共に条件を満たすとき、

$\forall \theta \in \mathbb{R}$, $T_n(\cos\theta) = \cos(n\theta) = t_n(\cos\theta)$

$\Rightarrow T_n(\cos\theta) - t_n(\cos\theta) = 0$

すると、z に関する方程式 $T_n(z) - t_n(z) = 0$ は無限個解を持つが、左辺が"恒等的に0"でなければ、この方程式の解の個数は左辺の次数以下で有限個より矛盾。

$\therefore T_n(z) - t_n(z) = 0 \Leftrightarrow T_n(z) = t_n(z)$ ■

この T_n を第1種チェビシェフ多項式という。

定理3. $n \in \mathbb{N}_0$ に対し、$\forall z \in \mathbb{C}$, $\sin z\, U_n(\cos z) = \sin(nz)$ なる整係数多項式 U_n が一意に存在する。

証明. 定理2同様。■

4. チェビシェフ多項式の関係

定理4. $n \in \mathbb{N}_0$ に対し、$\forall z \in \mathbb{C}$, $n U_n(z) = T_n'(z)$.

証明. $-\pi < \forall\theta < \pi$, $-n \sin\theta\, U_n(\cos\theta)$

$$= -n \sin(n\theta) = \frac{d(\cos(n\theta))}{d\theta}$$

$$= \frac{d(T_n(\cos\theta))}{d\theta}$$

$$= -\sin\theta\, T_n'(\cos\theta)$$

$$\Rightarrow n U_n(\cos\theta) - T_n'(\cos\theta) = 0$$

$(\because \sin\theta \neq 0)$

すると、z に関する方程式 $n U_n(z) - T_n'(z) = 0$ は無限個解をもつが、左辺が"恒等的に0"でなければ、この方程式の解の個数は左辺の次数以下で有限個より矛盾。

$\therefore n U_n(z) - T_n'(z) = 0 \Leftrightarrow n U_n(z) = T_n'(z)$ ■

U_n, T_n は整係数多項式なので、定理4より T_n' の各項の

係数は n の倍数で、このことにより T_n の各項の係数は n の倍数に準ずる整数であることが強く示唆される。

5. チェビシェフ多項式の係数

定理5. $T_n(z)$ $(n \in \mathbb{N}_0)$ の k 次 $(k \in \mathbb{N}_0)$ の項の係数は

$$\begin{cases} 0 & (2 \nmid n - k \text{ のとき}) \\ \dfrac{(-1)^{\frac{n-k}{2}}}{k!} \displaystyle\prod_{i=0}^{\frac{k}{2}-1} \left((n-2i)(n+2i)\right) & (2 \mid n, k \text{ のとき}) \\ \dfrac{(-1)^{\frac{n-k}{2}}}{k!} n \displaystyle\prod_{i=1}^{\frac{k-1}{2}} \left((n-2i+1)(n+2i-1)\right) & (2 \nmid n, k \text{ のとき}) \end{cases}$$

特に、$T_n(z)$ $(n \in \mathbb{Z}^+)$ の最高次の項の係数は $2^{n-1}z^n$

証明. n に関する帰納法により前半を示す。$n = 0, 1$ のとき、定理2 の議論より $T_0(z) = 1$, $T_1(z) = z$ よりよい。$n = m, m+1$ $(m \in \mathbb{N}_0)$ で成立つなら、$n = m+2$ のとき、定理2 の議論より

$$T_{m+2}(z) = 2zT_{m+1}(z) - T_m(z)$$

(1) $2 \nmid (m+2) - k$ のとき。

$2 \nmid (m+1) - (k-1)$, $2 \nmid m - k$ なので、$T_{m+2}(z)$ の k 次の項の係数は、帰納法の仮定より $2 \cdot 0 - 0 = 0$ よりよい。

(2) $2 \mid m+2$, $k = 0$ のとき

$2 \mid m, k$ なので、$T_{m+2}(z)$ の k 次の項の係数は、帰納法の仮定より

$$-\frac{(-1)^{\frac{m-k}{2}}}{k!} \prod_{i=0}^{\frac{k}{2}-1} \left((m-2i)(m+2i)\right)$$

$$= \frac{(-1)^{\frac{(m+2)-k}{2}}}{k!} \prod_{i=0}^{\frac{k}{2}-1} \left((m-2i)(m+2i)\right)$$

よりよい。

(3) $2 \mid m+2$, $k = 2$ のとき

$2 \nmid m+1, k-1$, $2 \mid m, k$ なので、$T_{m+2}(z)$ の k 次の項の係数は、帰納法の仮定より

$$2\cdot\frac{(-1)^{\frac{(m+1)-(k-1)}{2}}}{(k-1)!}(m+1)\prod_{i=1}^{\frac{(m+1)-(k-1)}{2}}\left(((m+1)-2i+1)((m+1)+2i-1)\right)-\frac{(-1)^{\frac{m-k}{2}}}{k!}\prod_{i=0}^{\frac{k}{2}-1}\left((m-2i)(m+2i)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\left(2\cdot 2(m+1)+m^2\right) \qquad (\because k=2)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}(m+2)^2$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=0}^{\frac{k}{2}-1}\left(((m+2)-2i)((m+2)+2i)\right) \qquad (\because k=2)$$

よりよい.

(4) $2\mid m+2,\ k,\ k\geqq 4$ のとき

$2\nmid m+1,\ k-1,\ 2\mid m,\ k$ であるので, $T_{m+2}(x)$ の k 次の項の係数は, 帰納法の仮定より

$$2\cdot\frac{(-1)^{\frac{(m+1)-(k-1)}{2}}}{(k-1)!}(m+1)\prod_{i=1}^{\frac{(k-1)-1}{2}}\left(((m+1)-2i+1)((m+1)+2i-1)\right)-\frac{(-1)^{\frac{m-k}{2}}}{k!}\prod_{i=0}^{\frac{k}{2}-1}\left((m-2i)(m+2i)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=1}^{\frac{k}{2}-1}(m+2i)\left(2k(m+1)\prod_{i=1}^{\frac{k}{2}-1}((m+2)-2i)+m\prod_{i=1}^{\frac{k}{2}}((m+2)-2i)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=1}^{\frac{k}{2}-1}((m+2)-2i)\prod_{i=0}^{\frac{k}{2}-2}((m+2)+2i)\left(2k(m+1)+m(m-k+2)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=1}^{\frac{k}{2}-1}((m+2)-2i)\prod_{i=0}^{\frac{k}{2}-2}((m+2)+2i)\left(m^2+km+2m+2k\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=1}^{\frac{k}{2}-1}((m+2)-2i)\prod_{i=0}^{\frac{k}{2}-2}((m+2)+2i)$$

$(m+k)(m+2)$

$$= \frac{(-1)^{\frac{(m+2)-k}{2}}}{k!} \prod_{i=0}^{\frac{k}{2}-1} \left(((m+2)-2i)((m+2)+2i)\right)$$

より成り。

(5) $2 \nmid m+2,\ k=1$ のとき

$2 \mid m+1,\ k-1,\ 2 \nmid m,\ k$ なので、$T_{m+2}(z)$ の k 次の項の係数は、帰納法の仮定より

$$2\cdot\frac{(-1)^{\frac{(m+1)-(k-1)}{2}}}{(k-1)!}\prod_{i=0}^{\frac{k-1}{2}-1}\left(((m+1)-2i)((m+1)+2i)\right)$$

$$-\frac{(-1)^{\frac{m-k}{2}}}{k!}\,m\prod_{i=1}^{\frac{k-1}{2}}\left((m-2i+1)(m+2i-1)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}(2\cdot 1+m) \qquad (\because k=1)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}(m+2)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}(m+2)\prod_{i=1}^{\frac{k-1}{2}}\left(((m+2)-2i+1)((m+2)+2i-1)\right) \qquad (\because k=1)$$

より成り。

(6) $2 \nmid m+2,\ k,\ k \geq 3$ のとき

$2 \mid m+1,\ k-1,\ 2 \nmid m,\ k$ なので、$T_{m+2}(z)$ の k 次の項の係数は、帰納法の仮定より

$$2\cdot\frac{(-1)^{\frac{(m+1)-(k-1)}{2}}}{(k-1)!}\prod_{i=0}^{\frac{k-1}{2}-1}\left(((m+1)-2i)((m+1)+2i)\right)$$

$$-\frac{(-1)^{\frac{m-k}{2}}}{k!}\,m\prod_{i=1}^{\frac{k-1}{2}}\left((m-2i+1)(m+2i-1)\right)$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}}{k!}\prod_{i=1}^{\frac{k-1}{2}-1}(m-2i+1)\{2k(m+1)$$

$$\prod_{i=0}^{\frac{k-1}{2}-1}((m+2)+2i-1)+m(m-k+2)\prod_{i=0}^{\frac{k-3}{2}}((m+2)+2i-1))$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}\prod_{i=2}^{\frac{k-1}{2}}((m+2)-2i+1)}{k!\prod_{i=0}^{\frac{k-3}{2}}((m+2)+2i-1)(2k(m+1)+m(m-k+2))}$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}\prod_{i=1}^{\frac{k-1}{2}}((m+2)-2i+1)}{k!\prod_{i=1}^{\frac{k-3}{2}}((m+2)+2i-1)(m^2+km+2m+2k)}$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}\prod_{i=1}^{\frac{k-1}{2}}((m+2)-2i+1)}{k!\prod_{i=1}^{\frac{k-3}{2}}((m+2)+2i-1)(m+k)(m+2)}$$

$$=\frac{(-1)^{\frac{(m+2)-k}{2}}(m+2)\prod_{i=1}^{\frac{k-1}{2}}((m+2)-2i+1)}{k!\prod_{i=1}^{\frac{k-1}{2}}((m+2)+2i-1)}$$

よりより。

よって、$T_n(z)$ の k 次の項の係数は主張の式になることが示された。すると、$n\in\mathbb{Z}^+$ のとき、$T_n(z)$ の $n+1$ 次以上の項の係数は主張の式より 0、n 次の項の係数は主張の式より $2\mid n$ のとき、

$$\frac{(-1)^{\frac{n-n}{2}}}{n!}\prod_{i=0}^{\frac{n}{2}-1}((n-2i)(n+2i))=\frac{1}{(n-1)!}\prod_{i=1}^{n-1}(2i)$$

$$=\frac{1}{(n-1)!}\cdot 2^{n-1}(n-1)!=2^{n-1},$$

$2 \nmid n$ のとき

$$\frac{(-1)^{\frac{n-n}{2}}}{n!} n \prod_{i=1}^{\frac{n-1}{2}} ((n-2i+1)(n+2i-1))$$

$$= \frac{1}{(n-1)!}\prod_{i=1}^{n-1}(2i) = \frac{1}{(n-1)!}\cdot 2^{n-1}(n-1)! = 2^{n-1}.$$

よって，$T_n(z)$ の最高次の項は $2^{n-1}z^n$ [redacted]

系 6. $\cos\frac{z}{n}, \cos\frac{z+2\pi}{n}, \cos\frac{z+4\pi}{n}, \dots, \cos\frac{z+2(n-1)\pi}{n}$ $(n\in\mathbb{Z}^+,\ z\in\mathbb{C})$ の k 次 $(1\le k\le n)$ 基本対称式は

$$\begin{cases} 0 & (2\nmid k<n \text{ のとき}) \\ \dfrac{\cos z}{2^{n-1}} & (2\nmid k=n \text{ のとき}) \\ \dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}(n-k)!}\displaystyle\prod_{i=0}^{\frac{n-k}{2}-1}((n-2i)(n+2i)) & (2\mid k<n,\ 2\mid n \text{ のとき}) \\ \dfrac{(-1)^{\frac{n}{2}}-\cos z}{2^{n-1}} & (2\mid k=n \text{ のとき}) \\ \dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}(n-k)!}\, n\displaystyle\prod_{i=1}^{\frac{n-k-1}{2}}((n-2i+1)(n+2i-1)) & (2\mid k,\ 2\nmid n \text{ のとき}) \end{cases}$$

証明. (1) $z\notin\pi\mathbb{Z}$ のとき

$$T_n\left(\cos\frac{z+2l\pi}{n}\right)-\cos z=\cos\left(n\cdot\frac{z+2l\pi}{n}\right)-\cos z=0$$

$(l=0,1,\dots,n-1)$ より，$w=\cos\frac{z+2l\pi}{n}$ $(l=0,1,\dots,n-1)$ は w に関する方程式 $T_n(w)-\cos z=0$ の解で，補題1.よりこれらは相異なる(∵ $0\le l<l'\le n-1$, $j\in\mathbb{Z}$ に対

$\frac{z+2l'\pi}{n} - \frac{z+2l\pi}{n} = \frac{l'-l}{n}\cdot 2\pi \notin 2\pi\mathbb{Z}$, $l, z \notin \pi\mathbb{Z}$ より

$z \neq (nj - l - l')\pi$

$\Rightarrow \frac{z+2l\pi}{n} + \frac{z+2l'\pi}{n} \neq 2j\pi$. よって、$\frac{z+2l\pi}{n} + \frac{z+2l'\pi}{n} \notin 2\pi\mathbb{Z}$) が、$w$ に関する n 次方程式 $T_n(w) - \cos z = 0$ の解は高々 n 個よりこれらのz。よって、解と係数の関係よりこれらの k 次基本対称式は定理5.より前述のようになる。

(2) $z \in 2\pi\mathbb{Z}$ のとき、

$\cos\frac{z}{n}$, $\cos\frac{z+2\pi}{n}$, $\cos\frac{z+4\pi}{n}$, …, $\cos\frac{z+2(n-1)\pi}{n}$ において各数が現れる回数は、$\cos 0$ が 1回、$\cos\frac{2l\pi}{n}$ $(l = 1, 2, \dots, [\frac{n}{2}] - 1)$ が 2回、$\cos\frac{2[\frac{n}{2}]\pi}{n}$ が $2\{\frac{n}{2}\}+1$ 回 ($\because z \in 2\pi\mathbb{Z}$) なので、これらの$k$次基本対称式を考えればよい。

$T_n\left(\cos\frac{2l\pi}{n}\right) - \cos z = \cos\left(n\cdot\frac{2l\pi}{n}\right) - 1 = 0$ $(l = 0, 1, \dots, [\frac{n}{2}])$,

$$\left.\frac{d(T_n(w) - \cos z)}{dw}\right|_{w=\cos\frac{2l\pi}{n}} = n U_n\left(\cos\frac{2l\pi}{n}\right) (\because 定理4)$$

$$= \frac{n\sin(n\cdot\frac{2l\pi}{n})}{\sin\frac{2l\pi}{n}} \quad (\because l = 1, 2, \dots, [\tfrac{n-1}{2}] \Rightarrow \sin\tfrac{2l\pi}{n} \neq 0)$$

$= 0$

$\left(l = 1, 2, \dots, \left[\frac{n-1}{2}\right]\right)$

より，$\left[\frac{n}{2}\right]+1$ 数 $w = \cos 0, \cos\frac{2l\pi}{n} \left(l = 1, 2, \dots, \left[\frac{n}{2}\right]-1\right), \cos\frac{2\left[\frac{n}{2}\right]\pi}{n}$ は相異なり，それぞれ w に関する方程式 $T_n(w) - \cos z = 0$ の高々単解，2重解，$2\left\{\frac{n}{2}\right\}+1$ 重解だが，w に関する n 次方程式 $T_n(w) - \cos z = 0$ の解は重複度を込めて n 個より それぞれ丁度単解，2重解，$2\left\{\frac{n}{2}\right\}+1$ 重解で，解はこれらのみ．よって，解と係数の関係より，これらの k 次基本対称式は定理5．より主張のようになる．

(3) $z \in \pi\mathbb{Z}$，$z \notin 2\pi\mathbb{Z}$ のとき．

(2) 同様．■

系7. $\sin\frac{z}{n}, \sin\frac{z+2\pi}{n}, \sin\frac{z+4\pi}{n}, \dots, \sin\frac{z+2(n-1)\pi}{n}$ $(n \in \mathbb{Z}^+, z \in \mathbb{C})$ の k 次 $(1 \leqq k \leqq n)$ 基本対称式は

$$\begin{cases} 0 & (2 \nmid k < n \text{ のとき}) \\ \dfrac{\cos\left(z - \frac{n\pi}{2}\right)}{2^{n-1}} & (2 \nmid k = n \text{ のとき}) \\ \dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}(n-k)!} \displaystyle\prod_{i=0}^{\frac{k}{2}-1} \left((n-2i)(n+2i)\right) & (2 \mid k < n,\ 2 \mid n \text{ のとき}) \\ \dfrac{(-1)^{\frac{n}{2}} - \cos\left(z - \frac{n\pi}{2}\right)}{2^{n-1}} & (2 \mid k = n \text{ のとき}) \end{cases}$$

$$\left\{\begin{array}{l}\dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}\cdot(n-k)!}\, n \displaystyle\prod_{i=1}^{\frac{n-k-1}{2}}\left((n-2i+1)(n+2i-1)\right) \\ (2|k,\ 2\nmid n \text{ のとき})\end{array}\right.$$

証明. $\sin\frac{z+2l\pi}{n} = \cos\frac{\left(z-\frac{n\pi}{2}\right)+2l\pi}{n}$ $(l=0,1,\dots,n-1)$

なので、系6で z を $z-\frac{n\pi}{2}$ で置き換えれば良い。■

系8. $U_n(z)$ $(n\in\mathbb{Z}^+)$ の k 次 $(k\in\mathbb{N}_0)$ の項の係数は

$$\begin{cases} 0 & (2|n-k \text{ のとき}) \\ \dfrac{(-1)^{\frac{n-k-1}{2}}}{k!\,n}\displaystyle\prod_{i=0}^{\frac{k-1}{2}}\left((n-2i)(n+2i)\right) & (2|n,\ 2\nmid k \text{ のとき}) \\ \dfrac{(-1)^{\frac{n-k-1}{2}}}{k!}\displaystyle\prod_{i=1}^{\frac{k}{2}}\left((n-2i+1)(n+2i-1)\right) & (2\nmid n,\ 2|k \text{ のとき}) \end{cases}$$

特に、$U_n(z)$ $(n\in\mathbb{Z}^+)$ の最高次の項の係数は $2^{n-1}z^{n-1}$

証明. 定理4より、求める係数は $T_n(z)$ の $k+1$ 次の項の係数の $\frac{k+1}{n}$ 倍なので定理5より示された。■

系9. $\cos\frac{\pi}{n}, \cos\frac{2\pi}{n}, \dots, \cos\frac{(n-1)\pi}{n}$ $(n\in\mathbb{Z}^+)$ の k 次 $(1\le k\le n-1)$ 基本対称式は

$$\begin{cases} 0 & (2\nmid k \text{ のとき}) \\ \dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}(n-k-1)!\,n}\displaystyle\prod_{i=0}^{\frac{n-k}{2}-1}\left((n-2i)(n+2i)\right) & (2|n,\ 2|k \text{ のとき}) \\ \dfrac{(-1)^{\frac{k}{2}}}{2^{n-1}(n-k-1)!}\displaystyle\prod_{i=1}^{\frac{n-k-1}{2}}\left((n-2i+1)(n+2i-1)\right) & (2\nmid n,\ 2|k \text{ のとき}) \end{cases}$$

証明. $U_n\left(\cos\frac{l\pi}{n}\right) = \frac{\sin\left(n\cdot\frac{l\pi}{n}\right)}{\sin\frac{l\pi}{n}}$ $\left(\because l=1,2,\dots,n-1 \Rightarrow \sin\frac{l\pi}{n}\neq 0\right)$

$=0\ (l=1,2,\cdots,n-1)$ で，$\cos\frac{\pi}{n}, \cos\frac{2\pi}{n}, \cdots, \cos\frac{(n-1)\pi}{n}$ は相異なるが，z に関する $n-1$ 次方程式 $U_n(z)=0$ の解は高々 $n-1$ 個よりこれらのみ．よって，解と係数の関係よりこれらの k 次基本対称式は系8.より主張のようになる．■

この系をもう少し拡張したかったが，$U_n(\cos z)=\frac{\sin(nz)}{\sin z}$ $(\sin z \neq 0)$ という条件は，右辺が0でないとき非常に扱いづらく，本質的に上と同じ場合しか示せなかった．

6. おまけ

因みに，チェビシェフ多項式に注目すれば，ある種の数の無理性も簡単に示せる．以下 $\mathbb{Q}$, $\mathbb{R}$ でそれぞれ有理数，実数の集合を表す．

全単射 $[0,\pi]\to[-1,1]$, $x\mapsto\cos x$ の逆写像を Arccos，

$\left[-\frac{\pi}{2},\frac{\pi}{2}\right]\to[-1,1]$, $x\mapsto\sin x$ の逆写像を Arcsin，$\left(-\frac{\pi}{2},\frac{\pi}{2}\right)\to\mathbb{R}$, $x\mapsto\tan x$

の逆写像を Arctan とかく．又，以下では，代数の分野でのある程度の知識は黙って用いる．

定理10．（$\mathbb{Q}$上）代数的な $\alpha\in[-1,1]$ が虚数と $\mathbb{Q}$ 上共役なら，$\frac{\mathrm{Arccos}\,\alpha}{\pi}\notin\mathbb{Q}$．

証明．$\frac{\mathrm{Arccos}\,\alpha}{\pi}\in\mathbb{Q}$ と仮定すると，$\frac{\mathrm{Arccos}\,\alpha}{\pi}=\frac{n}{m}$ $(m,$

$n \in \mathbb{Z},\ m > 0$)とおける. 仮定より, αの最小多項式をfとおけ, 又αと共役な虚数βがとれる. このとき

$T_{2m}(\alpha) = T_{2m}(\cos(\mathrm{Arccos}\,\alpha)) = \cos(2m\,\mathrm{Arccos}\,\alpha) = \cos(2n\pi) = 1$

$\therefore T_{2m}(\alpha) - 1 = 0$

$\Leftrightarrow f(x) \mid T_{2m}(x) - 1$

$\Rightarrow T_{2m}(\beta) - 1 = 0 \qquad (\because f(\beta) = 0)$

$\Leftrightarrow 0 \leqq {}^{\exists}l \leqq m,\ \beta = \cos\dfrac{2l\pi}{2m} \qquad$ ($\because$系6.の議論)

で, 左辺は虚数, 右辺は実数より矛盾. よって示された. ■

例 $\alpha = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ ($p_1, p_2, \cdots, p_n$は素数, $p_1 < p_2 < \cdots < p_n$, $e_1, e_2, \cdots, e_n \in \mathbb{Q}$, $2e_1, 2e_2, \cdots, 2e_n \notin \mathbb{Z}$, $0 < \alpha < 1$)の$\mathbb{Q}$上最小多項式は$x^N - \alpha^N$

$(N \geqq 3)$の形より, $(e^{\frac{2\pi i}{N}}\alpha)^N - \alpha^N = 0$なので$\alpha$は虚数$e^{\frac{2\pi i}{N}}\alpha$と共役. $\therefore$定理10.より$\dfrac{\mathrm{Arccos}\,\alpha}{\pi} \notin \mathbb{Q}$. 又

, $\dfrac{\mathrm{Arccos}(-\alpha)}{\pi} = -\dfrac{\mathrm{Arccos}\,\alpha}{\pi} \notin \mathbb{Q}$.

定理10.のαに対し, $\dfrac{\mathrm{Arcsin}\,\alpha}{\pi} = \dfrac{\frac{\pi}{2} - \mathrm{Arccos}\,\alpha}{\pi}$

$= \dfrac{1}{2} - \dfrac{\mathrm{Arccos}\,\alpha}{\pi} \notin \mathbb{Q}$ ($\because$定理10)から最左辺の無理性も分かる. 又, $\alpha \in \mathbb{R}$のとき$\theta := \mathrm{Arctan}\,\alpha$とおくと,

$\tan\theta = \alpha$

$\Rightarrow \sin\theta = \alpha\cos\theta$ ―①

$\Rightarrow (1 + \alpha^2)\cos^2\theta = \cos^2\theta + \sin^2\theta = 1$

$\Rightarrow \cos\theta = \dfrac{1}{\sqrt{1+\alpha^2}} \qquad (\because -\frac{\pi}{2} < \theta < \frac{\pi}{2}$より$\cos\theta > 0)$

$$\Rightarrow \sin\theta = \frac{\alpha}{\sqrt{1+\alpha^2}}$$
$$\Leftrightarrow \theta = \mathrm{Arcsin}\frac{\alpha}{\sqrt{1+\alpha^2}}$$

より, $\dfrac{\mathrm{Arctan}\alpha}{\pi} = \dfrac{\mathrm{Arcsin}\frac{\alpha}{\sqrt{1+\alpha^2}}}{\pi}$ の無理性は上の議論から分かることがある.

7　おわりに

いかがでしたか. この記事は, 昨年考え, 和田杯にも出題した*1内容を部誌用に書いたものです. 実際に書いてみると着想の部分よりも帰納法を回す面倒な部分が大半を占めてしまいましたが, 大目に見ていただければと思います. 去年考えていたこの内容以外にも考えていたことはあったのですが, 準備期間の短さの為にこの記事を載せることとなってしまいました. 来年はもう少し精進したいと思います. それでも, 少し非自明な主張が出来たのは嬉しかったです.

また,6 章の後付け感が否めないですが, 例えば急に $\dfrac{\mathrm{Arccos}\frac{1}{\sqrt[3]{2}}}{\pi}$ の無理性を示すよう言われたところで自分にはすぐには示せないでしょうから, それはそれでよいものと考えております.

今後の展望としては, 系 9 のさらなる拡張が考えられます. 文化祭後も考えていきたいと思います.

この記事にも必ず誤植があるでしょうが, 大したことがなければお許し下さい.

最後になりますが, ここまで拙い記事をお読みいただき有り難うございました. 他の記事も是非お読みになって下さい.

参考文献

なし

*1 解説当日は, 解説用ノートを忘れてわけのわからない解説をしてしまい, 申し訳ございませんでした.