

代数学の基本定理 まとめノート

Takahiro Nukui

平成 27 年 2 月 28 日

目 次

1	はじめに	2
2	複素数 (2 章)	3
2.1	演習問題 2.8	3
3	多項式と複素多項式 (3 章)	5
3.1	補題 3.2.1 の証明 (p30)	5

1 はじめに

このまとめノートは「代数学の基本定理」(共立出版 著者: Benjamin Fine、Gerhard Rosenberger、訳者: 新妻弘、木村哲三)の中の難しそうな演習問題や定理の証明の補足などをまとめたものです。平成 27 年 2 月 28 日現在、この本を用いてほそぼそと勉強会を開いているので、ご興味のある方はどなたでもご連絡ください。一緒に読んでいきましょう!

2 複素数 (2 章)

2.1 演習問題 2.8

演習問題 2. 8 の回答を記す。そのために 4 つの公理を提示し、それらが互いに等しいことを証明する¹。

すべての数を A, B の二組に分けて、 A に属する各数を B に属する各数よりも小さくすることができたとするとき、このような組み分け、 (A, B) を**切断**といい、 A を下組、 B を上組という。

公理：Dedekind の定理

実数の切断は、下組と上組との境界として、一つの数を確認する。

補足

すなわち、切断 (A, B) が与えられた時、一つの数 s が存在して、 s は A の最大数または B の最小数であり、前者では B に最小数はなく、後者では A に最大数がない。

集合 S に属する数がすべて一つの数 M よりも大でないときには、 S は上方に有界であるといい、 M をその一つの上界という。式で書くと

$$\exists M \in \mathbb{R}, \forall x \in S [x \leq M] \iff S \text{ は上方に有界}$$

上界の集合に最小元が存在すれば、それを上限と呼ぶ。

公理：Weierstrass の定理

数の集合 S が上方 [または下方] に有界ならば、 S の上限 [または下限] が存在する。

”Dedekind の定理 \implies Weierstrass の定理”の証明

S は上方に有界であると仮定して、上限の存在を証明する。

S は上方に有界なので、以下のような空でない集合 A が取れ²、 A 以外の実数の全てを B とする。

$$A = \{x | \forall y \in S [y \leq x]\}$$

$$B = \mathbb{R} \setminus A = \{x | \exists y \in S [x < y]\}$$

任意の A の元の値は、任意の B の元の値以上になっているので、 A と B は実数の切断になっている。Dedekind の定理によって、 A と B の境界となる s が存在する。

$s \in B$ とすると、

$$\exists a \in S \quad [s < a]$$

このような a と s の中間点にある一つの数 b ($s < b < a$) とすると、 b は a よりも小さいので上界ではない ($x \notin A$)。また s よりも大きいので $x \notin B$ 。よって矛盾。

結局、 $s \in A$ が示される。 s は上界の集合の中で最小なので、上限である。 S が下方に有界の場合も同様に示される。(証明終了)

¹主に [2] を参考にした。

²このような $x \in A$ が上界の定義である

公理：有界な単調数列の収束

有界な単調数列は収束する。

”Weierstrass の定理 \implies 有界な単調数列の収束”の証明

数列 a_n が有界で、広義に単調増加するとする。つまり

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq \cdots$$

で、任意の n に関して $a_n \leq M$ なる定数 M が存在する。

Weierstrass の定理により、 $\{a_n\}$ の集合には、上限 α が存在する。 α が上限であることと、 $\{a_n\}$ が単調増加することから、

$$\forall \alpha' < \alpha, \exists n_0 [n \geq n_0 \Rightarrow \alpha' < a_n]$$

$\alpha - \alpha' = \epsilon$ とみれば、

$$\forall \epsilon > 0, \exists n_0 [n \geq n_0 \Rightarrow \epsilon > \alpha - a_n]$$

となり、 $\{a_n\}$ が α に収束することが示された。(証明終了)

公理：区間縮小法の原理

$\{I_n\}$ が $I_{n+1} \subset I_n$ を満たす閉区間の列で、その区間の長さが 0 に収束するならば、すべての区間に共通なただ一つの点 x_0 が存在する。

”有界な単調数列の収束 \implies 区間縮小法の原理”の証明

$I_n = [a_n, b_n]$ とすると、

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq \cdots \leq b_n \leq \cdots \leq b_2 \leq b_1$$

すなわち、数列 $\{a_n\}, \{b_n\}$ は単調でかつ有界である。有界な単調数列は収束するので、

$$\lim_{n \rightarrow \infty} a_n = \alpha, \quad \lim_{n \rightarrow \infty} b_n = \beta$$

となる α と β が存在する。区間の長さが 0 に収束することから $\alpha = \beta$ 。

任意の n に関して $a_n \leq \alpha \leq b_n$ だから、 α はすべての区間に属する。また、 α が $\{a_n\}$ の上限、 $\{b_n\}$ の下限であることから、 α 以外に各区間に共通な点は存在しない。(証明終了)

最後に区間縮小法の原理から Dedekind の公理を導けば、4つの公理がすべて同値であることが示せる。

”区間縮小法の原理 \implies Dedekind の公理”の証明

(A, B) を実数の切断とする。 A, B から一対の数 a_0, b_0 を取り出して、区間 $[a_0, b_0]$ を I_0 と名付ける。以下

$$I_n = [a_n, b_n]$$
$$a_{n+1} = \begin{cases} a_n & (\frac{a_n+b_n}{2} \in B \text{ のとき}) \\ \frac{a_n+b_n}{2} & (\frac{a_n+b_n}{2} \in A \text{ のとき}) \end{cases}$$
$$b_{n+1} = \begin{cases} \frac{a_n+b_n}{2} & (\frac{a_n+b_n}{2} \in B \text{ のとき}) \\ b_n & (\frac{a_n+b_n}{2} \in A \text{ のとき}) \end{cases}$$

このように、区間を定義すれば、 $\{I_n\}$ が $I_{n+1} \subset I_n$ を満たし、その区間の長さが 0 に収束するので、区間縮小法の原理により、ただ一つの点 x_0 が存在する。この x_0 は A と B の境界になっている。(証明終了)

3 多項式と複素多項式 (3 章)

3.1 補題 3.2.1 の証明 (p30)

補題 3.2.1

$f(x), g(x) \in F[x]$ とする。このとき、 $f(x)$ と $g(x)$ の最大公約数はただ一つ存在する。それは $f(x)$ と $g(x)$ の一次結合で表されているものの中で最小の次数をもつモニックな多項式である。

証明

ユークリッドの互除法の操作は必ず終了し、かつ唯一の答えを返すので、最大公約数はただ一つ存在する。以下では、「 $f(x)$ と $g(x)$ の一次結合で表されているものの中で最小の次数をもつモニックな多項式」が最大公約数であることを証明する。 $d(x)$ を、 $f(x)$ と $g(x)$ の一次結合で表されているものの中で最小の次数をもつモニックな多項式とする。つまり、以下のように表現出来る。

$$d(x) = f(x)h(x) + g(x)k(x)$$

(ただし $h(x), k(x) \in F[x]$)

$f(x)$ を $d(x)$ で割った余りが $r(x)$ であるとする、

$$f(x) = d(x)q(x) + r(x)$$

そのため、

$$\begin{aligned} r(x) &= f(x) - d(x)q(x) \\ &= f(x) - \{f(x)h(x) + g(x)k(x)\}q(x) \\ &= f(x)\{1 - h(x)q(x)\} + g(x)\{-k(x)q(x)\} \end{aligned}$$

$r(x)$ は $d(x)$ で割った余りなので、 $\deg r(x) < \deg d(x)$ のはずだが、 $d(x)$ は $f(x)$ と $g(x)$ の一次結合で表されているものの中で最小の次数を持つ多項式なので、 $r(x) = 0$ である。よって、 $d(x)$ は $f(x)$ を割り切る。 $g(x)$ を割り切ることも同様に証明可能。(証明終了)

参考文献

- [1] Benjamin Fine、Gerhard Rosenberger、(訳) 新妻弘、木村哲三, “代数学の基本定理”, 共立出版 (2002).
- [2] 高木貞治, “解析概論” 岩波書店 (2010)