代数学の基本定理のいろんな証明

北窓 @seasawher

January 5, 2021

今から何をするか

このスライドの目的は, 次の代数学の基本定理の証明をなるべくたくさん紹介することです

代数学の基本定理

定数でない n 次多項式 $f \in \mathbb{C}[z]$ に対して, $f(z) = 0$ となる複素数 z が少なくともひとつ存在する.

ここでは予備知識を補うことはできませんでしたが, 雰囲気だけでも感じとっていただけたらと思います.

目次

証明法 1 - k 乗根の存在から

要旨

ハイリホーによる. 定数でない n 次多項式 f に対して, その絶対値を返す関数 $g(z) = |f(z)|$ を考える. g の最小値を $g(c)$ とする. このとき, $g(c) > 0$ であると仮定すると, c を $\mathbb{C}$ 上で少しずらすことにより $g(z)$ の値をより小さくできることがわかる. これは c の取り方に矛盾する.

この証明で使用している多項式と $\mathbb{C}$ の性質

- $x^k - \alpha$ には $\mathbb{C}$ 上で根がある
- 多項式は連続である
- 多項式 $f(z)$ は $|z| \to \infty$ のとき絶対値が無限大になる

証明-最小値の存在

まず $g(z)$ の最小値が存在することを示そう. $|z| \to \infty$ のとき $g(z) \to \infty$ なので, ある R が存在して

$$|z| \geq R \Rightarrow g(z) \geq g(0)$$

が成り立つ. ここで $D_R = \{z \in \mathbb{C} \mid |z| \leq R\}$ はコンパクトで g は連続なので, g は D_R 上で最小値を持つ. それを $g(c)$ としよう. R の定義から, $g(c)$ は $\mathbb{C}$ 上でも最小値になっている.

以降 $g(c) > 0$ と仮定する.

証明-k 乗根をとる

f を点 c を中心に展開すると次のように表せる.

$$f(z) = f(c) + a_1(z-c) + a_2(z-c)^2 + \cdots + a_n(z-c)^n$$

そこに $z = c + y$ を代入して

$$f(c+y) = f(c) + a_1 y + a_2 y^2 + \cdots + a_n y^n$$

を得る. f は定数ではないと仮定したので, 係数 a_i がすべてゼロということはない. $a_i \neq 0$ となるような最小の添え字 i を k とおく. そうすると, ある多項式 $p \in \mathbb{C}[y]$ によって

$$f(c+y) = f(c) + a_k y^k + y^{k+1} p(y)$$

と表せる. ここで複素数の範囲では k 乗根がとれることを用いて, $f(c) + a_k \beta^k = 0$ となる $\beta \in \mathbb{C} \setminus \{0\}$ をとる.

証明-g(c) より小さい値を構成する

実数 $t \in [0,1]$ をとり c を β の方向にずらした点での値を計算する. y に $t\beta$ を代入すると

$$f(c+t\beta) = (1-t^k)f(c) + t^{k+1}\beta^{k+1}p(t\beta)$$

となる. $E = \max_{t\in[0,1]} \left|\beta^{k+1}p(t\beta)\right|$ とおく. 絶対値をとると

$$g(c+t\beta) \leq (1-t^k)g(c) + t^{k+1}E$$

である. これは書き換えると

$$\begin{aligned} g(c+t\beta) - g(c) &\leq -t^k g(c) + t^{k+1}E \\ &\leq t^k(E\cdot t - g(c)) \end{aligned}$$

とも表せる. 右辺を $h(t)$ とおく.
$E=0$ なら h は $t>0$ 上で負になる. $E>0$ なら, h は $0<t<g(c)/E$ において負になる. いずれにせよ, ある $0<t_0\leq 1$ が存在して $h(t_0)<0$ である. このとき $g(c+t_0\beta)-g(c)\leq h(t_0)<0$ である. これは $g(c)$ が g の最小値として取られていたことに反しており, 矛盾.

証明法 2 - 円周の基本群が自明でないことから

要旨

ハイリホーによる. r を固定するごとに, $f(re^{2\pi\sqrt{-1}\theta})$ は閉曲線を定める. ここで $r = 0$ とすると定値写像であるが, 十分大きい R に対して $r = R$ とすると $f(Re^{2\pi\sqrt{-1}\theta})$ は原点を n 周する曲線になっている. $f(re^{2\pi\sqrt{-1}\theta})$ は r に関して連続なので, $\mathbb{C} \setminus \{0\}$ の中で原点を回る曲線を連続的に動かして一点に縮められるということになるが, これは（どう頑張っても穴に引っかかるので）不可能である.

この証明で使用している多項式と $\mathbb{C}$ の性質

- $\mathbb{C} \setminus \{0\} \simeq S^1$ の基本群は曲線 $e^{2\pi\sqrt{-1}\theta}$ の同値類で生成される自由 Abel 群
- 多項式は連続である
- $|z|$ が十分大きいとき $f(z)$ の値はほぼ最高次の z^n の項だけで決定される

証明-下準備

円周 $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ の基本群についての有名な定理 $\pi_1(S^1) \cong \mathbb{Z}$ に帰着したいので, そのために多少の工夫をする.
閉曲線の族 $G_r \colon [0,1] \to S^1$ を

$$G_r(\theta) = \frac{f(re^{2\pi\sqrt{-1}\theta})}{\left|f(re^{2\pi\sqrt{-1}\theta})\right|}$$

と定めると, これで $\mathbb{C} \setminus \{0\}$ から S^1 に帰着できる.
しかし, 基本群に帰着するためには基点がないといけないので, これだと少しまずい. 点 $G_0 = f(0)/|f(0)|$ をすべての G_r が通るというわけではないからである.
そこで閉曲線の族 $F_r \colon [0,1] \to S^1$ を

$$F_r(\theta) = \frac{f(re^{2\pi\sqrt{-1}\theta})/f(r)}{\left|f(re^{2\pi\sqrt{-1}\theta})/f(r)\right|}$$

と定める. このようにしておくと, どんな $r \geq 0$ についても $F_r(0) = 1$ である.

証明-直観的説明

有理関数は分母がゼロでないところでは連続なので F_r は連続で, F はホモトピーになっている.
$F_0 = 1$ であり, 一方で十分大きい r について $F_r(\theta)$ はほとんど $e^{2\pi\sqrt{-1}n\theta}$ と同じといっていいので, 定数 1 を S^1 上で連続的に動かして原点を n 周する閉曲線に重ねることができるということになる.
しかし S^1 のようなドーナツ型の穴の開いた空間の上ではそんなことは不可能なので, これは矛盾である.

要旨にも書いたこの直観的な説明は正しいが,
「r が大きいところでは f はほぼ z^n である」というのはきちんと正当化しないといけない.

証明-z^n へのホモトピーの構成

$f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$ と表されていたとしよう.
以下, r を $\max\{1, |a_1| + \cdots + |a_n|\}$ よりも大きくすればよいことを確かめる.

$R > \max\{1, |a_1| + \cdots + |a_n|\}$ なる実数 R をとって固定したとする. いま $|z| = R$ とすると

$$\begin{aligned} |z^n| &> (|a_1| + \cdots + |a_n|) \left|z^{n-1}\right| \\ &> \left|a_1 z^{n-1}\right| + \left|a_2 z^{n-2}\right| + \cdots + |a_n| \\ &\geq \left|a_1 z^{n-1} + \cdots + a_n\right| \end{aligned}$$

である. したがって任意の $t \in [0, 1]$ について

$$f_t(z) = z^n + t(a_1 z^{n-1} + \cdots + a_n)$$

は $|z| = R$ 上で根を持たない. これは $z^n \simeq f(z)$ という C_R から $\mathbb{C} \setminus \{0\}$ への写像の間のホモトピーを構成したことになる.

証明-結び

閉曲線 F_R の式における $f(z) = f_1(z)$ を $z^n = f_0(z)$ で置き換える. そうすると, $F_R(\theta)$ は $e^{2\pi\sqrt{-1}n\theta}$ になる. すなわち, 曲線 $F_R(\theta)$ は $e^{2\pi\sqrt{-1}n\theta}$ とホモトピー同値である.
ここまでくると, 「自然数 n に対して曲線 $\theta \mapsto e^{2\pi\sqrt{-1}\theta}$ のホモトピー類を対応させる写像が $\mathbb{Z}$ から $\pi_1(S^1)$ への同型写像である」という代数トポロジーの定理が使えるようになった.
今更であるが $\gamma(\theta) = e^{2\pi\sqrt{-1}\theta}$ とおき, ホモトピー類を括弧 $[,]$ であらわすことにする. そうすると $\pi_1(S^1)$ の元として

$$0 = [F_0] = [F_R] = n[\gamma]$$

が成り立つことになる. $\pi_1(S)$ は自由 Abel 群なので $[\gamma] = 0$ ということになり, 矛盾.

証明法 3 - Liouville の定理から

要旨

ハイリホーによる.f が $\mathbb{C}$ 上に根を持たないと仮定する. このとき $g(z) = 1/f(z)$ は有界で, かつ全平面で正則である. したがって Liouville の定理により, g は定数でなければならない. これは矛盾.

この証明で使用している多項式と $\mathbb{C}$ の性質

- 有理関数は分母がゼロになる点を除いた領域で正則
- $|z| \to \infty$ のとき $|f(z)| \to \infty$

証明

$|z| \to \infty$ のとき $|f(z)| \to \infty$ なので, ある実数 R であって, $|z| \geq R$ ならば $|f(z)| \geq 1$ となるものがとれる. このとき閉円盤 D_R の外側で g は有界.
また $|f|$ は連続なのでコンパクト集合 D_R の中で最小値 ε をとる. f が根を持たないという仮定より, $\varepsilon > 0$ である. よって g は D_R の中でも有界で, したがって $\mathbb{C}$ 全体で有界.

よって Liouville の定理により g は定数関数でなければならないが, これは矛盾である.

証明法 4-Cauchy の積分定理から

要旨

$f \in \mathbb{R}[x]$ と仮定しても一般性を失わない．ハイリホーによる．$1/f(2\cos\theta)$ の区間 $I = [0, 2\pi]$ 上での積分を考える．f に根がないことから，f の符号は正か負のどちらかに偏るので，この定積分はゼロにはならない．一方で，$z = e^{i\theta}$ として変数変換するとこれは単位円周 C 上での正則な関数の積分になり，Cauchy の積分定理からその値はゼロ．これは矛盾である．

この証明で使用している多項式と $\mathbb{C}$ の性質

- 有理関数は分母がゼロになる点を除いた領域で正則
- f が多項式なら $g(z) = z^n f(z + z^{-1})$ も多項式になる

証明-下準備

$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ とする. f の係数の複素共役をとったものを $\overline{f}$ と表す. すなわち

$$\overline{f}(z) = z^n + \overline{a_{n-1}}z^{n-1} + \cdots + \overline{a_1}z + \overline{a_0}$$

である. $F(z) = f(z)\overline{f}(z)$ とすると, F の係数はすべて実数であり, しかも $F(z) = 0$ ならば $f(z)f(\overline{z}) = 0$ が成り立つ. したがって, はじめから f は実数係数だとしてよい.

証明-積分への帰着

さて, $f \in \mathbb{R}[x]$ が複素数の根を持たないと仮定する. f は実数の根も持たないので, f は実数上で常に正であるか負であるかのどちらかである. f はもちろん連続なので, したがって

$$J := \int_0^{2\pi} \frac{d\theta}{f(2\cos\theta)} \neq 0$$

が成り立つ. この積分において $z = e^{i\theta}$ と変数変換する. そうすると

$$2\cos\theta = z + z^{-1} \qquad d\theta = \frac{dz}{iz}$$

なので, 単位円周を C とすれば

$$J = \frac{1}{i} \int_C \frac{dz}{zf(z + z^{-1})}$$

であるということになる.

証明-結び

これは $g(z) := z^n f(z + z^{-1})$ とおくと次のようにも表せる.

$$J = \frac{1}{i} \int_C \frac{z^{n-1}}{g(z)}\, dz$$

ここで g はやはり多項式であり, $g(0)$ が f の最高次の係数に等しく, したがってゼロではないことに注意すると g は $\mathbb{C}$ 上に根を持たないことがわかる.
よって g は C 上とその内部 (を含む適当な領域) で正則であり, ゆえに Cauchy の積分定理から, $J = 0$ でなければならない. これは矛盾である.

証明法 5-Galois 理論から

要旨

$\mathbb{C}$ が代数閉体であることを示す.

この証明で使用している多項式と $\mathbb{C}$ の性質

- 奇数次数の実数係数多項式 $f \in \mathbb{R}[x]$ は必ず $\mathbb{R}$ に根を持つ
- 2 次方程式には解の公式がある

証明-拡大次数が 2 のベキの場合に帰着

ハイリホーで示す. $\mathbb{C}$ が代数閉体でないと仮定し, $\mathbb{C}$ の有限次拡大 $L \neq \mathbb{C}$ が存在したとする. 適当に Galois 閉包を取ることにより, $L/\mathbb{C}$ は Galois 拡大だとしてよい.

Step 1

$[L : \mathbb{C}]$ は 2 のベキである.

$G = \mathrm{Gal}(L/\mathbb{R})$ の Sylow 2-部分群 H をとる. H の不変体を M としよう. そうすると Galois の基本定理により $[M : \mathbb{R}] = |G/H|$ は奇数である.
$M/\mathbb{R}$ は有限次分離拡大なので, 単拡大である. よってある $\alpha \in M$ が存在して, $M = \mathbb{R}[\alpha]$ とかける. α の $\mathbb{R}$ 上の最小多項式を $g \in \mathbb{R}[x]$ とする. このとき g は既約だが, 奇数次数の実数係数多項式は必ず実数に根を持つので, g の次数は 1 でなければならない. よって $M = \mathbb{R}$ なので $G = H$ の位数は 2 のベキ. よって $[L : \mathbb{R}]$ も 2 のベキである.
$[L : \mathbb{C}]$ は $[L : \mathbb{R}]$ を割り切るので, とくに $[L : \mathbb{C}]$ も 2 のベキである.

証明-Abel 拡大なら矛盾

Step 2

$L/\mathbb{C}$ が Abel 拡大なら, 矛盾にぶちあたる.
拡大次数が 2 のベキであるような $\mathbb{C}$ の Abel 拡大は存在しない.

$L/\mathbb{C}$ が Abel 拡大だったとする. このとき有限生成 Abel 群の基本定理から, $G^* = \mathrm{Gal}(L/\mathbb{C})$ には指数 2 の部分群 J が存在する. J の不変体を W としよう. このとき Galois の基本定理により $[W : \mathbb{C}] = |G^*/J| = 2$ である. よって W は $\mathbb{C}$ 上の二次多項式のある根によって生成されていることになる.
ところが 2 次方程式には解の公式があったわけだから, これは矛盾である.

証明-Abel 拡大でなくても矛盾

Step 3

$L/\mathbb{C}$ が Abel 拡大でなくても, やはり矛盾に突き当たる.

$G^* = \mathrm{Gal}(L/\mathbb{C})$ の交換子群 $Z = [G^*, G^*]$ を考える. Z の不変体を M とする. (Step 1 とは違う M) $Z \triangleleft G^*$ なので, $M/\mathbb{C}$ は Galois 拡大である. このとき $\mathrm{Gal}(M/\mathbb{C}) \cong G^*/Z$ なので, M は $\mathbb{C}$ の Abel 拡大になっている. かつ, その拡大次数は 2 のベキまたは 1 である. よって Step 2 により $M = \mathbb{C}$ でなくてはならない.
これにより $Z = G^*$ つまり G^* がその交換子群と等しいことが導かれるが, これは G^* が p 群であることに矛盾する. (G^* の位数についての帰納法による. 確かめよ)

参考文献

いずれの方法も誰が最初に考えたものなのかは私は知りません．どの手法も私のオリジナルのものではありません．このスライドを作成するにあたって参考にしたものをここに書きます．

- 代数学の基本定理とその初等的な証明 / 高校数学の美しい物語
  https://mathtrain.jp/algebrabasic
- Allen Hatcher「Algebraic Topology」
  著者の HP から無料公開されてるので興味があればぜひ．
  http://pi.math.cornell.edu/~hatcher/AT/ATpage.html
- チャーチル, ブラウン「複素関数入門」数学書房
- 雪江明彦「代数学 2 環と体とガロア理論」日本評論社