乗法的情報による加法構造の復元

星 裕一郎 (京都大学 数理解析研究所)

目次

1 数や式に対する加法 · 乗法

まず最初に, 基本的な記号を導入しましょう. 整数 (例えば, 1 や 0 や -2 などといった数のことです) 全体のなす集合を $\mathbb{Z}$ と書くことにします. 有理数 ($= \dfrac{\text{整数}}{0\text{でない整数}}$ と書ける数のことで, 例えば, $\dfrac{1}{7}$ や $-\dfrac{3}{2}$ などのことです; 任意の整数 n は $\dfrac{n}{1}$ とも書けますので, すべての整数は有理数です) 全体のなす集合を $\mathbb{Q}$ と書くことにします. 複素数 (例えば, $\sqrt{2}$ や円周率 π や $1+\sqrt{-1}$ などといった数のことです; すべての有理数は複素数です) 全体のなす集合を $\mathbb{C}$ と書くことにします.

$$\mathbb{Z} \overset{\text{def}}{=} \{\, \text{整数} \,\} \subseteq \mathbb{Q} \overset{\text{def}}{=} \{\, \text{有理数} \,\} \subseteq \mathbb{C} \overset{\text{def}}{=} \{\, \text{複素数} \,\}$$

さて, こういった数に対するもっとも基本的な操作として, “加法 (=足し算)” と “乗法 (=掛け算)” があります. 上で定めた 3 つの集合 $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ のいずれに対しても, その中で, 通常の加法や乗法を自由に行うことができます. つまり, 2 つの整数の和 (あるいは積) はやはり整数ですし, 2 つの有理数の和 (あるいは積) はやはり有理数ですし, 2 つの複素数の和 (あるいは積) はやはり複素数となります. この加法 · 乗法という 2 つの操作は, 非常に複雑に絡み合っており, 例えば整数に関わる様々な問題の難しさは, ある意味において, この複雑な絡み合いに起因していると考えられます.

まず最初に, 有理数の加法と乗法の関わりの理解の困難さを, “素因数分解” という具体的かつ初等的な枠組みを通じて観察しましょう. 0 でない整数に対して, 素因数分解というものを考えることができます. 即ち, 0

でない整数 $n \in \mathbb{Z}$ に対して, 相異なる素数 $p_1, \ldots, p_r$ と正整数 $d_1, \ldots, d_r$ と $\epsilon \in \{1, -1\}$ が存在して,

$$n \;=\; \epsilon \cdot p_1^{d_1} \cdots p_r^{d_r}$$

となります. また, 上で述べたとおり, 有理数とは整数の比として得られる数のことですので, 0 でない有理数に対しても, 素因数分解というものを考えることができます. 即ち, 0 でない有理数 $q \in \mathbb{Q}$ に対して, 相異なる素数 $p_1, \ldots, p_r$ と 0 でない整数 $d_1, \ldots, d_r$ と $\epsilon \in \{1, -1\}$ が存在して,

$$q \;=\; \epsilon \cdot p_1^{d_1} \cdots p_r^{d_r}$$

となります. 例えば, $\dfrac{5}{3} = 1 \cdot 3^{-1} \cdot 5$, $-\dfrac{36}{1145} = -1 \cdot 2^2 \cdot 3^2 \cdot 5^{-1} \cdot 229^{-1}$ が素因数分解の例です. この “素因数分解” の持つ重要な性質として, 以下の 2 つの性質が挙げられます.

(a)　0 でない有理数 $q \in \mathbb{Q}$ に対して, その素因数分解を $q = \epsilon \cdot p_1^{d_1} \cdots p_r^{d_r}$ と書くと, 組のなす集合 $\{(p_1, d_1), \ldots, (p_r, d_r)\}$ と $\epsilon \in \{1, -1\}$ は q より一意的に定まる. また, 逆に, この集合 $\{(p_1, d_1), \ldots, (p_r, d_r)\}$ と $\epsilon \in \{1, -1\}$ によって元々の有理数 q は完全に決定される. 上の例を用いて説明すると,

$$\frac{5}{3} \;\leftrightarrow\; \big(\{(3,-1),(5,1)\},1\big),$$

$$-\frac{36}{1145} \;\leftrightarrow\; \big(\{(2,2),(3,2),(5,-1),(229,-1)\},-1\big)$$

という対応において, 左側から右側が復元可能, また, 右側から左側が復元可能.

(b)　0 でない 2 つの有理数 $q, q' \in \mathbb{Q}$ に対して, q と q' のそれぞれの素因数分解から, 積 $q \cdot q'$ の素因数分解を簡単に与えることができる. その手続きの厳密な詳細は省略するが, 上の例を用いて説明すると,

$$\frac{5}{3} = 1 \cdot 3^{-1} \cdot 5, \quad -\frac{36}{1145} = -1 \cdot 2^2 \cdot 3^2 \cdot 5^{-1} \cdot 229^{-1}$$

という素因数分解から, 積 $\dfrac{5}{3} \cdot -\dfrac{36}{1145}$ $\left(= -\dfrac{180}{3435} = -\dfrac{12}{229}\right)$ の素因数分解は以下のように簡単に計算可能.

$$\frac{5}{3} \cdot -\frac{36}{1145} \;=\; 1 \cdot 3^{-1} \cdot 5 \cdot -1 \cdot 2^2 \cdot 3^2 \cdot 5^{-1} \cdot 229^{-1} = -1 \cdot 2^2 \cdot 3^1 \cdot 229^{-1}.$$

つまり, (a) で議論された対応

$$\frac{5}{3} \;\leftrightarrow\; \big(\{(3,-1),(5,1)\},1\big),$$

$$-\frac{36}{1145} \;\leftrightarrow\; \big(\{(2,2),(3,2),(5,-1),(229,-1)\},-1\big)$$

の右側のみから, 対応の左側の積として得られる有理数の素因数分解を記述することが容易に可能.

$$\big(\{(3,-1),(5,1)\},1\big), \quad \big(\{(2,2),(3,2),(5,-1),(229,-1)\},-1\big) \quad \rightsquigarrow \quad \big(\{(2,2),(3,1),(229,-1)\},-1\big).$$

性質 (a) は, “素因数分解とは, 有理数のある適切な整理の方法である” ということを意味していると考えられます. そして, この視点に立ちますと, 性質 (b) は, “素因数分解という有理数の整理の方法は, 乗法と非常に相性が良い”, もっと踏み込んだ表現をするならば,

> 素因数分解とは, 有理数の乗法的な理解そのものである

ということを主張していると考えられると思います.

数の管理, ラベリングの方法:

従来型: ..., 4, 5, 6, 7, 8, 9, 10, ...

素因数分解型: ..., $\{(2,2)\}$, $\{(5,1)\}$, $\{(2,1),(3,1)\}$, $\{(7,1)\}$, $\{(2,3)\}$, $\{(3,2)\}$, $\{(2,1),(5,1)\}$, ...

(“ϵ 部分” はすべて 1 なので省略)

乗法:

従来型: $2 \cdot 5 = 10, \quad 6 \cdot 9 = 54$

素因数分解型: $\{(2,1)\} \cdot \{(5,1)\} = \{(2,1),(5,1)\}, \quad \{(2,1),(3,1)\} \cdot \{(3,2)\} = \{(2,1),(3,3)\}$

(従来型への移行の必要はない!)

素因数分解型の数の管理

一方, この “有理数の乗法的な理解そのもの” であるところの “素因数分解” と, “加法” はどのように関連しているでしょうか. 私にとっての答えを述べてしまいますと, “少なくとも私には簡単な関係は見い出せない” となります. 実際, 例えば, いくつかの簡単な足し算の式

$$4 + 9 = 13, \quad 5 + 7 = 12, \quad 12 + 16 = 28$$

を素因数分解の表示で書くと

$$2^2 + 3^2 = 13^1, \quad 5^1 + 7^1 = 2^2 \cdot 3, \quad 2^2 \cdot 3 + 2^4 = 2^2 \cdot 7$$

となりますが, 左辺の分解の様子から右辺の分解の様子を想像することは, まったく容易ではないと言えると思います. つまり, 有理数を素因数分解型の表示で表したとき, その和を, 従来型への移行なくして記述することは, 非常に困難だということです. このように, “数の乗法的な整理の方法” である “素因数分解” は, 加法と相性が良いとは言い難いものとなっています. こういった議論から, 加法と乗法の関連はそう簡単に理解できるものではない, ということがおわかりいただけるかと思います.

また, 加法と乗法の関連の難しさの別の例として, Fermat 予想[*1]が挙げられると思います. Fermat 予想とは, 以下の主張が正しいであろうという予想です.

3 以上の整数 $n \in \mathbb{Z}$ と有理数 $a, b, c \in \mathbb{Q}$ に対して, もしも $a^n + b^n = c^n$ ならば, $abc = 0$.

与えられた有理数に対して, それがある有理数の n 乗として得られる, という性質は, 乗法的に簡単に定義される, そして, 比較的珍しい性質です. この視点に立ちますと, Fermat 予想の主張とは, “そのような乗法的な比較的珍しい性質を有する 2 つの数の和が再びその乗法的な比較的珍しい性質を有することは, 当たり前な場合を除いて起こり得ない” という, 乗法と加法の間のある関連についてのものだと考えられます. そして, 乗法と加法の関連についてのこの予想が非常に難しい問題であったという歴史的事実をご存知の方も少なくないと思います.

さて, これまで議論してきた “加法” や “乗法” は所謂 “数” に対してのみ定義されるものではありません.

[*1] 2007 年に, この数学入門公開講座で, 安田正大さん (現 · 大阪大学) が, “$R = T$ 定理の仕組みとその応用” という演題で, この Fermat 予想に関する講義を行いました. その際のテキストは, 数理解析研究所のホームページから入手することが可能です.

例えば, “式” に対しても, 加法や乗法が定義されます. ここで, 本講義で議論の中心となるタイプの “式” を定義しておきましょう. x をその変数として, 複素数 $a_0, \dots, a_n \in \mathbb{C}$ を用いて

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

と書ける式のことを, **(複素数係数) 多項式** と呼び, その全体のなす集合を $\mathbb{C}[x]$ と書きます. 具体的には, 例えば,

$$x, \quad x+1, \quad x^2+2x+1, \quad 84x^{2014}$$

などが多項式です. (少なくとも) a_0 を除いた係数がすべて 0 の場合だと考えることによって, 複素数も多項式だと見做すことができます.

$$\mathbb{C} \ \subseteq \ \mathbb{C}[x] \ \stackrel{\text{def}}{=} \ \{\text{(複素数係数) 多項式 }\}.$$

また, 整数をもとに有理数を定義する方法を多項式に適用することによって, $\dfrac{\text{多項式}}{0 \text{ でない多項式}}$ と書ける式を考えることができます. このような式のことを, **(複素数係数) 有理式** と呼び, その全体のなす集合を $\mathbb{C}(x)$ と書きます. 具体的には, 例えば,

$$\frac{x}{x+1}, \quad \frac{84x^{2014}}{x^2+2x+1}$$

などが有理式です. 整数を有理数と見做す方法と同様の方法によって (つまり, 分母を 1 だと考えることによって), 多項式もやはり有理式と見做すことができます.

$$\mathbb{C}[x] \ \subseteq \ \mathbb{C}(x) \ \stackrel{\text{def}}{=} \ \{\text{(複素数係数) 有理式 }\}.$$

本講義の主役は, この有理式となります. また, これら多項式や有理式に対して, 普通の意味の加法や乗法が定義できることは皆さんご存知だと思います. 形式的にその厳密な定義を書くこともできますが, そんなことをしなくても, 以下のようないくつかの例で確認をすれば, 一般的な場合においてもその具体的な実行方法を想像できると思います.

$$(x+1)+(x^2+2x+1) \ = \ x+1+x^2+2x+1 \ = \ x^2+(1+2)x+(1+1) \ = \ x^2+3x+2,$$

$$\frac{x}{x+1}+\frac{84x^{2014}}{x^2+2x+1} \ = \ \frac{x(x+1)}{(x+1)^2}+\frac{84x^{2014}}{(x+1)^2} \ = \ \frac{x(x+1)+84x^{2014}}{(x+1)^2} = \ \frac{84x^{2014}+x^2+x}{x^2+2x+1},$$

$$(x+1)\cdot(x^2+2x+1) \ = \ x\cdot(x^2+2x+1)+1\cdot(x^2+2x+1) = \ (x^3+2x^2+x)+(x^2+2x+1) \ = \ x^3+3x^2+3x+1,$$

$$\frac{x}{x+1}\cdot\frac{84x^{2014}}{x^2+2x+1} \ = \ \frac{x\cdot 84x^{2014}}{(x+1)\cdot(x^2+2x+1)} \ = \ \frac{84x^{2015}}{x^3+3x^2+3x+1}.$$

また, この “式” に対する加法や乗法も, 先ほど議論した “数” に対するそれと同様, 容易には理解し難い, 複雑な結び付き, 絡み合いを有しています.

一方, その絡み合いの 1 つの表れとして, 数や式の適当な集まりに対して, そこで定義される加法を, その乗法的な情報によって記述 · 復元することができる場合があります. 本講義では, そのようなタイプの数学的命題について, お話をしようと思います. 特に, 本講義の目標であるところの定理の主張を大雑把に述べるならば,

$\mathbb{C}(x)$ のある乗法的な情報から, その加法を復元 · 記述するある手続きが存在する

となります. そのもう少し正確な主張については, §3 の冒頭をご参照ください. 今回の講義では, 時間の都合により, それについて詳しく議論をすることはできませんが, この定理には, “有理数版” も存在します. 有理数の方が有理式よりも身近で, その分その主張を説明することが容易ですので, 以下でその “有理数版” のもう少し正確な主張を述べることで, 本講義の目標である定理の雰囲気を感じ取っていただきましょう.

すべての素数のなす集合を $\mathfrak{Primes}$ と書くことにします.

$$\mathfrak{Primes} \stackrel{\text{def}}{=} \{ \text{素数} \} = \{2, 3, 5, 7, 11, 13, 17, 19, ...\}.$$

また, 各素数 $p \in \mathfrak{Primes}$ に対して, $\mathbb{Q}$ の部分集合

$$\mathbb{Z}_{(p)}^{=1} \subseteq \mathbb{Z}_{(p)}^{\triangleright} \subseteq \mathbb{Q}$$

を, 以下のように定義します.

- $\mathbb{Z}_{(p)}^{\triangleright} \subseteq \mathbb{Q}$ を, 0 でない有理数 $q \in \mathbb{Q}$ であって, q を $q = \epsilon \cdot \dfrac{n}{m}$, ただし, $\epsilon \in \{1, -1\}$, n と m は 1 以外に公約数を持たない正整数, と書いたとき, m が p を約数として持たないもの全体のなす集合とする.
- $\mathbb{Z}_{(p)}^{=1} \subseteq \mathbb{Q}$ を, 0 でない有理数 $q \in \mathbb{Q}$ であって, q を $q = \epsilon \cdot \dfrac{n}{m}$, ただし, $\epsilon \in \{1, -1\}$, n と m は 1 以外に公約数を持たない正整数, と書いたとき, $\epsilon \cdot n$ を p で割った余りと m を p で割った余りが等しいもの全体のなす集合とする.

例えば, 有理数 $-\dfrac{36}{1145}$ の場合,

- 分母 1145 の素因数は 5 と 229 のみなので,

  $p \neq 5, 229$ のときには $-\dfrac{36}{1145} \in \mathbb{Z}_{(p)}^{\triangleright}$, また, $-\dfrac{36}{1145} \notin \mathbb{Z}_{(5)}^{\triangleright}, \mathbb{Z}_{(229)}^{\triangleright}$,

- 分子 -36 と分母 1145 をそれぞれ割って余りが等しくなる素数は 1181 のみなので,

  $-\dfrac{36}{1145} \in \mathbb{Z}_{(1181)}^{=1}$, また, $p \neq 1181$ のときには $-\dfrac{36}{1145} \notin \mathbb{Z}_{(p)}^{=1}$,

となります.

この記号の準備のもと, 主定理の “有理数版” のもう少し正確な主張は, 以下のようになります.

主定理の “有理数版”　集合 $\mathbb{Q}$ と $\mathfrak{Primes}$ が与えられたとき,

(1)　$\mathbb{Q}$ の乗法構造

$$\begin{array}{ccc} \mathbb{Q} \times \mathbb{Q} & \longrightarrow & \mathbb{Q} \\ (q, q') & \mapsto & q \cdot q', \end{array}$$

(2)　$\mathfrak{Primes}$ の元で添字付けられた $\mathbb{Q}$ の部分集合の族

$$\left\{ \mathbb{Z}_{(p)}^{=1} \subseteq \mathbb{Z}_{(p)}^{\triangleright} \subseteq \mathbb{Q} \right\}_{p \in \mathfrak{Primes}}$$

という情報から, $\mathbb{Q}$ の加法構造

$$\begin{array}{ccc} \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{Q} \\ (q, q') & \mapsto & q+q' \end{array}$$

を記述する手続きが存在する.

§1 の最後に, こういったタイプの数学的命題たちに関する簡単な歴史を述べましょう. こういった内容の定理は, その起源を [6] に求めることができると思います. [6] では, 所謂 “関数体に対する Neukirch · 内田の定理” という定理—その当時そういった枠組みはありませんでしたが, 現代的表現を用いれば, “有限体上の代数曲線に対する Grothendieck による遠アーベル予想の双有理版”—を証明するために, 本講義の主結果のようなタイプの結果が用いられています. また, [6] で用いられたその結果は, [2] に “Proposition 1.3” として, 簡潔に纏められています. [6], [2] のどちらを見てもわかりますが, この復元の手続きは, 今回の講義で議論する “複素数係数有理式全体” という式の集まりに対してのみ適用されるべきものではなく, より一般に, “代数的閉体上の代数曲線の関数体” という式の集まりがその適用対象となっています. そして, 式の集まりに対する加法構造の復元手続きに関するこの結果は, 順番に, [5], [3], [4] という論文の中で, 改良され, そして, 進化しています. 一方, すぐ上で述べた “有理数版” ですが, これは [1] の中で議論されています. [1] においては, 所望の結果を “手続き的な形式” では述べていませんが, その議論を適切に処理することによって, “手続き的な形式” による結果に書き換えることが可能です. また, [1] で得られている結果も, 先の “式” に対するそれと同様, “有理数全体” という数の集まりに対してのみ適用されるべきものではなく, より一般に, “数体” という数の集まりがその適用の対象となっています.

2　有理式に付随する様々な乗法的概念

この §2 では, §1 でその定義を復習した “有理式” に付随する様々な概念を導入しましょう.

定義 2.1.

(i)　0 でない多項式 $f(x) \in \mathbb{C}[x]$ に対して, $f(x)$ が

$$f(x) \ = \ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

ただし, $a_0, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, と書けるとき,

$$\deg(f(x)) \stackrel{\text{def}}{=} \ n \ \in \ \mathbb{Z}$$

と定義する.

(ii)　0 でない有理式 $Q(x) \in \mathbb{C}(x)$ に対して, $Q(x)$ が

$$Q(x) \ = \ \frac{f(x)}{g(x)},$$

ただし, $f(x)$, $g(x) \in \mathbb{C}[x]$, $g(x) \neq 0$, $f(x)$ と $g(x)$ は共通因子を持たない (つまり, 2 つの方程式 $f(x) = 0$ と $g(x) = 0$ が共通解を持たない), と書けるとき,

$$\deg(Q(x)) \stackrel{\text{def}}{=} \ \deg(f(x)) - \deg(g(x)) \ \in \ \mathbb{Z}$$

と定義する.

定数的でない多項式 $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$ を与えますと, 複素数のなす集合 $\mathbb{C}$ のよく知られた性質によって, 方程式 $f(x) = 0$ は常に (複素数) 解を持ちます. 特に, 多項式 $f(x)$ は適当な複素数 $a \in \mathbb{C}$ による $x - a$ という多項式をその因子として持ちます. 即ち, ある多項式 $g(x) \in \mathbb{C}[x]$ が存在して, $f(x) = (x - a) \cdot g(x)$ と書くことができます. このとき, 当然 $\deg(g(x)) = \deg(f(x)) - 1$ となりますので, “deg” に関する帰納法により, 以下の命題を証明することができます.

命題 2.2. 0 でない多項式 $f(x) \in \mathbb{C}[x]$ に対して, 相異なる複素数 $a_1, \ldots, a_n \in \mathbb{C}$, 正整数 $d_1, \ldots, d_n \in \mathbb{Z}$, 0 でない複素数 $c \in \mathbb{C}$ が存在して, 等式

$$f(x) \ = \ c \cdot (x - a_1)^{d_1} \cdots (x - a_n)^{d_n}$$

が成立する. また, 集合 $\{(a_1, d_1), \ldots, (a_n, d_n)\}$ は $f(x)$ より一意的に定まる.

命題 2.2 で与えられている等式は, 多項式に対する “整数の素因数分解” の類似と考えられます.
有理式とは多項式の比として得られる式のことですので, 命題 2.2 より, 以下の命題が得られます.

命題 2.3. 0 でない有理式 $Q(x) \in \mathbb{C}(x)$ に対して, 相異なる複素数 $a_1, \ldots, a_n \in \mathbb{C}$, 0 でない整数 $d_1, \ldots, d_n \in \mathbb{Z}$, 0 でない複素数 $c \in \mathbb{C}$ が存在して, 等式

$$Q(x) \ = \ c \cdot (x - a_1)^{d_1} \cdots (x - a_n)^{d_n}$$

が成立する. また, 集合 $\{(a_1, d_1), \ldots, (a_n, d_n)\}$ は $Q(x)$ より一意的に定まる.

命題 2.3 で与えられている等式は, 有理式に対する “有理数の素因数分解” の類似と考えられます. また, 命題 2.2 では d_i たちは “正整数” ですが, 命題 2.3 では “0 でない整数” となっていることに注意しましょう. 具体的な例を与えますと, 例えば, $\dfrac{5x+5}{x^3-14x^2+49x}$ という有理式は,

$$\frac{5x+5}{x^3-14x^2+49x} \;=\; \frac{5(x+1)}{x(x-7)^2} \;=\; 5\cdot(x+1)^1\cdot x^{-1}\cdot(x-7)^{-2}$$

と “素因数分解” できます.

$Q(x)\in\mathbb{C}(x)$ を 0 でない有理式とします. このとき, 命題 2.3 によって $\{(a_1,d_1),\dots,(a_n,d_n)\}$ という集合を定めることができます. 一方, 命題 2.3 で与えられている表示から簡単にわかるとおり, この集合 $\{(a_1,d_1),\dots,(a_n,d_n)\}$ によって元々の有理式 $Q(x)$ は “0 でない複素数倍” を除いて一意的に決定されます. この観察から, 集合 $\{(a_1,d_1),\dots,(a_n,d_n)\}$ は有理式 $Q(x)$ に対する非常に重要な情報であることがわかると思います. 上で挙げた例 $\dfrac{5x+5}{x^3-14x^2+49x}$ で説明するならば, 件の集合は

$$\{(-1,1),(0,-1),(7,-2)\}$$

となり, この集合から, もとの有理式が

$$?\cdot(x-(-1))^1\cdot(x-0)^{-1}\cdot(x-7)^{-2} \;=?\cdot\frac{x+1}{x(x-7)^2}=?\cdot\frac{x+1}{x^3-14x^2+49x}$$

というように, “0 でない複素数倍” を除いて決定されます.

さて, この重要な情報 “$\{(a_1,d_1),\dots,(a_n,d_n)\}$” と等価と考えられる “ord” という概念を, 以下のように定義しましょう.

定義 2.4. 0 でない有理式 $Q(x)\in\mathbb{C}(x)$ と複素数 $a\in\mathbb{C}$ に対して,

$$\mathrm{ord}_a(Q(x)) \;\in\; \mathbb{Z}$$

を以下のように定義する. $Q(x)=c\cdot(x-a_1)^{d_1}\cdots(x-a_n)^{d_n}$ を 命題 2.3 で与えられた $Q(x)$ の表示としたとき,

(1)　もしも $a\notin\{a_1,\dots,a_n\}$ ならば $\mathrm{ord}_a(Q(x))\overset{\mathrm{def}}{=}0$,

(2)　もしもある $1\le i\le n$ が存在して $a=a_i$ が成立するならば, $\mathrm{ord}_a(Q(x))\overset{\mathrm{def}}{=}d_i$.

(2) の場合に関する注意ですが, $a_1,\dots,a_n$ は相異なる複素数ですので, ある $1\le i\le n$ が存在して $a=a_i$ が成立しますと, i とは異なる $1\le j\le n$ に対して $a=a_j$ が成立することはない, ということに注意しましょう. また, すべての複素数 $a\in\mathbb{C}$ に対する $\mathrm{ord}_a(Q(x))$ たちを考えれば, 先の集合 “$\{(a_1,d_1),\dots,(a_n,d_n)\}$” を復元することができることは容易に確認できると思います. 上で挙げた例 $\dfrac{5x+5}{x^3-14x^2+49x}$ の場合, その有理式の “素因数分解” から,

$$\mathrm{ord}_{-1}\Big(\frac{5x+5}{x^3-14x^2+49x}\Big) \;=\; 1,\quad \mathrm{ord}_0\Big(\frac{5x+5}{x^3-14x^2+49x}\Big) \;=\; -1,$$

$$\mathrm{ord}_7\Big(\frac{5x+5}{x^3-14x^2+49x}\Big) \;=\; -2,\quad \mathrm{ord}_z\Big(\frac{5x+5}{x^3-14x^2+49x}\Big) \;=\; 0\quad(\forall z\in\mathbb{C}\setminus\{-1,0,7\})$$

となります.

定義 2.5. $Q(x) \in \mathbb{C}(x)$ を 0 でない有理式, $a \in \mathbb{C}$ を複素数とする. 不等式 $\mathrm{ord}_a(Q(x)) > 0$ が成立するとき, a は $Q(x)$ の **零点** であると言う. 不等式 $\mathrm{ord}_a(Q(x)) < 0$ が成立するとき, a は $Q(x)$ の **極** であると言う.

従って, 上で挙げた例 $\dfrac{5x+5}{x^3-14x^2+49x}$ の場合, -1 がその零点であり, そして, 0 と 7 がその極となります. 簡単に確認できるとおり, a が $Q(x)$ の極であるときには, $Q(x)$ に a を代入しようとすると "$\dfrac{0 \text{ でない値}}{0}$" となってしまい, つまり (普通の意味では) 代入はできません. 逆に, a が $Q(x)$ の極でなければ, $Q(x)$ に a を代入することができ, $Q(a) \in \mathbb{C}$ という複素数が得られます. また, 再び簡単に確認できるように, a が $Q(x)$ の極でないとしますと, $Q(a) = 0$ となることと, a が $Q(x)$ の零点であることは同値です.

定義 2.6. 複素数 $a \in \mathbb{C}$ に対して, $\mathbb{C}(x)$ の部分集合

$$\mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x)$$

を以下のように定義する.

$$\mathcal{O}_a^{\times} \stackrel{\text{def}}{=} \{\, Q(x) \in \mathbb{C}(x) \setminus \{0\} \,|\, \mathrm{ord}_a(Q(x)) = 0 \,\}$$
$$\subseteq \mathcal{O}_a^{\triangleright} \stackrel{\text{def}}{=} \{\, Q(x) \in \mathbb{C}(x) \setminus \{0\} \,|\, \mathrm{ord}_a(Q(x)) \geq 0 \,\}.$$

つまり, $\mathcal{O}_a^{\times} \subseteq \mathbb{C}(x)$ は "a を零点としても極としても持たない有理式全体" で, $\mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x)$ は "a を極として持たない有理式全体" です. すぐ上の観察から, $\mathcal{O}_a^{\triangleright}$ に属する有理式には a を代入することができます. ここで, 折角 "代入" という操作を観察したところですので, この代入によって定義される簡単な概念を導入しましょう.

定義 2.7. 複素数 $a \in \mathbb{C}$ に対して, $\mathbb{C}(x)$ の部分集合

$$\mathcal{O}_a^{=1} \subseteq \mathbb{C}(x)$$

を以下のように定義する.

$$\mathcal{O}_a^{=1} \stackrel{\text{def}}{=} \{\, Q(x) \in \mathcal{O}_a^{\triangleright} \,|\, Q(a) = 1 \,\}.$$

つまり, $\mathcal{O}_a^{=1} \subseteq \mathbb{C}(x)$ は "a を代入すると 1 となる有理式全体" です. $\mathcal{O}_a^{=1}$ に属する有理式に a を代入すると 1 になるのですから, 特に, $\mathcal{O}_a^{=1}$ に属する有理式は a を零点としても極としても持ちません. 従って, $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times}$ となります.

次に, 後々の話の都合上, これまでに複素数 $a \in \mathbb{C}$ に対して定義した ord_a, $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ という概念を, "∞" という点に対しても定義したいと思います.

定義 2.8.

(i)　0 でない有理式 $\mathbb{Q}(x) \in \mathbb{C}(x)$ に対して,

$$\mathrm{ord}_{\infty}(Q(x)) \stackrel{\text{def}}{=} -\deg(Q(x))$$

と定義する.

(ii)　$\mathbb{C}(x)$ の部分集合

$$\mathcal{O}_{\infty}^{\times} \subseteq \mathcal{O}_{\infty}^{\triangleright} \subseteq \mathbb{C}(x)$$

を以下のように定義する.

$$\mathcal{O}_{\infty}^{\times} \stackrel{\text{def}}{=} \{\, Q(x) \in \mathbb{C}(x) \setminus \{0\} \,|\, \mathrm{ord}_{\infty}(Q(x)) = 0 \,\}$$

$$\subseteq\ \mathcal{O}_\infty^{\triangleright}\ \stackrel{\text{def}}{=}\ \{\,Q(x)\in\mathbb{C}(x)\setminus\{0\}\,|\,\mathrm{ord}_\infty(Q(x))\geq 0\,\}.$$

(iii)　$Q(x)\in\mathcal{O}_\infty^{\triangleright}$ に対して, 複素数 $Q(\infty)\in\mathbb{C}$ を, 以下のように定義する.

(1)　$Q(x)\notin\mathcal{O}_\infty^{\times}$ (つまり, $\mathrm{ord}_\infty(Q(x))>0$) ならば, $Q(\infty)\stackrel{\text{def}}{=}0$.

(2)　$Q(x)\in\mathcal{O}_\infty^{\times}$ (つまり, $\mathrm{ord}_\infty(Q(x))=0$) ならば, $Q(x)=c\cdot(x-a_1)^{d_1}\cdots(x-a_n)^{d_n}$ を命題 2.3 で与えられた表示とすると, $Q(\infty)\stackrel{\text{def}}{=}c$.

(iv)　$\mathbb{C}(x)$ の部分集合

$$\mathcal{O}_\infty^{=1}\ \subseteq\ \mathbb{C}(x)$$

を以下のように定義する.

$$\mathcal{O}_\infty^{=1}\ \stackrel{\text{def}}{=}\ \{\,Q(x)\in\mathcal{O}_\infty^{\times}\,|\,Q(\infty)=1\,\}$$

$=\{\,Q(x)\in\mathcal{O}_\infty^{\times}\,|\,Q(x)=c\cdot(x-a_1)^{d_1}\cdots(x-a_n)^{d_n}$を命題2.3で与えられた表示としたとき, $c=1\,\}$.

(v)　0 でない有理式 $Q(x)\in\mathbb{C}(x)$ に対して, 不等式 $\mathrm{ord}_\infty(Q(x))>0$ が成立するとき, ∞ は $Q(x)$ の **零点** であると言う. 不等式 $\mathrm{ord}_\infty(Q(x))<0$ が成立するとき, ∞ は $Q(x)$ の **極** であると言う.

ここで,

$$\mathbb{P}^1\ \stackrel{\text{def}}{=}\ \mathbb{C}\cup\{\infty\}$$

と書くことにします. これまでに議論よって, 任意の $a\in\mathbb{P}^1$ に対して,

0 でない有理式 $Q(x)\in\mathbb{C}(x)$ に対して,　$Q(x)\in\mathcal{O}_a^{\triangleright}\ \Leftrightarrow\ \mathrm{ord}_a(Q(x))\geq 0\ \Leftrightarrow$　$Q(x)$ に a を代入可能

$Q(x)\in\mathcal{O}_a^{\triangleright}$ に対して,　$Q(x)\notin\mathcal{O}_a^{\times}\ \Leftrightarrow\ \mathrm{ord}_a(Q(x))>0\ \Leftrightarrow\ Q(a)=0\ \Leftrightarrow$　a は $Q(x)$ の零点

という関係が存在することに注意しましょう.

次に, “∞” という点に対しても適切に “ord” を定義した恩恵と考えられる以下の命題を確認します.

命題 2.9. 0 でない有理式 $Q(x)\in\mathbb{C}(x)$ に対して, 有限部分集合 $S\subseteq\mathbb{P}^1$ が存在して, $a\notin S$ ならば $\mathrm{ord}_a(Q(x))=0$. また, 等式

$$\sum_{a\in\mathbb{P}^1}\mathrm{ord}_a(Q(x))\ =\ 0$$

が成立する.

証明は簡単です. 主張の前半部分は命題 2.3 の表示から直ちに従います. また, 再び命題 2.3 の表示と, そして, 複素数 $a\in\mathbb{C}$ に対する ord_a の定義から,

$$\sum_{a\in\mathbb{C}}\mathrm{ord}_a(Q(x))\ =\ \deg(Q(x))$$

が容易に確認できますので, 残っている ord_∞ の定義から, 主張の後半部分の等式が従います.

この §2 では, 有理式に関する概念として, 任意の $a\in\mathbb{P}^1$ に対して,

$$\mathrm{ord}_a,\quad \mathcal{O}_a^{=1}\ \subseteq\ \mathcal{O}_a^{\times}\ \subseteq\ \mathcal{O}_a^{\triangleright}$$

を定義してきました. §2 の最後に, これらの概念について, この講義の観点から非常に重要な事実を観察しましょう. それは,

> ord_a, $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ は, 乗法との相性は良いが, 加法との相性は良くない

という事実です. 別の言い方をしますと,

> ord_a, $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ は, 加法的な概念ではなく乗法的な概念である

という事実です. 乗法との相性の良さについては, 以下の命題がそれを支持しています.

命題 2.10. $a \in \mathbb{P}^1$ とする.

(i)　0 でない有理式 $Q(x)$, $P(x) \in \mathbb{C}(x)$ に対して, 等式

$$\mathrm{ord}_a(Q(x)\cdot P(x)) \;=\; \mathrm{ord}_a(Q(x)) + \mathrm{ord}_a(P(x)), \quad \mathrm{ord}_a(Q(x)^{-1}) \;=\; -\mathrm{ord}_a(Q(x))$$

が成立する.

(ii)　$Q(x)$, $P(x) \in \mathcal{O}_a^{=1}$ ならば, $Q(x)\cdot P(x) \in \mathcal{O}_a^{=1}$, $Q(x)^{-1} \in \mathcal{O}_a^{=1}$ が成立する.

(iii)　$Q(x)$, $P(x) \in \mathcal{O}_a^{\times}$ ならば, $Q(x)\cdot P(x) \in \mathcal{O}_a^{\times}$, $Q(x)^{-1} \in \mathcal{O}_a^{\times}$ が成立する.

(iv)　$Q(x)$, $P(x) \in \mathcal{O}_a^{\triangleright}$ ならば, $Q(x)\cdot P(x) \in \mathcal{O}_a^{\triangleright}$ が成立する.

まずその証明を与えてしまいましょう. (i) は "ord_a" の定義から簡単に確認できますので, 演習問題としましょう. (iv) は (i) と $\mathcal{O}_a^{\triangleright}$ の定義から直ちに従います. 実際, $Q(x)$, $P(x) \in \mathcal{O}_a^{\triangleright}$ ならば, $\mathcal{O}_a^{\triangleright}$ の定義から, $\mathrm{ord}_a(Q(x))$, $\mathrm{ord}_a(P(x)) \geq 0$ となりますので, (i) より $\mathrm{ord}_a(Q(x)\cdot P(x)) = \mathrm{ord}_a(Q(x)) + \mathrm{ord}_a(P(x)) \geq 0$ となり, 再び $\mathcal{O}_a^{\triangleright}$ の定義から, $Q(x)\cdot P(x) \in \mathcal{O}_a^{\triangleright}$ が成立します. (iii) も (iv) の証明とほとんど同様の議論から得られます. (ii) を証明するために, $Q(x)$, $P(x) \in \mathcal{O}_a^{=1}$ としましょう. すると, (iii) より, $Q(x)\cdot P(x)$, $Q(x)^{-1} \in \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ となりますので, 特に, $Q(x)\cdot P(x)$ や $Q(x)^{-1}$ に a を代入することが可能です. そして, 実際に $Q(x)\cdot P(x)$ に a を代入してみますと, その値は $Q(a)\cdot P(a) = 1\cdot 1 = 1$ となり, $Q(x)\cdot P(x) \in \mathcal{O}_a^{=1}$ が確認できますし, また, $Q(x)^{-1}$ に a を代入してみますと, その値は $Q(a)^{-1} = 1^{-1} = 1$ となり, やはり $Q(x)^{-1} \in \mathcal{O}_a^{=1}$ が確認できます.

命題 2.10 の内容ですが, まず, (i) の帰結としまして

> $\mathrm{ord}_a(Q(x)\cdot P(x))$ を $\mathrm{ord}_a(Q(x))$ と $\mathrm{ord}_a(P(x))$ のみから計算することができる

という観察が得られます. つまり, 2 つの有理式の積の "ord_a" による値は, 元々の 2 つの有理式の "ord_a" による値たちから完全に決定される, ということです. 一方, (ii), (iii), (iv) は

> $\mathcal{O}_a^{=1}$, $\mathcal{O}_a^{\times}$, $\mathcal{O}_a^{\triangleright}$ のいずれに対しても, その中で自由に乗法ができる

という主張を含んでいます.

一方, ord_a, $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ といった対象が, 加法とは相性が良くないという主張を, 以下の例で観察しましょう. 加法に対する命題 2.10 の類似は成立しないことが以下の例でわかります.

- $\mathrm{ord}_a(Q(x))$ と $\mathrm{ord}_a(P(x))$ のみから $\mathrm{ord}_a(Q(x)+P(x))$ を計算することはできない. 実際, 例えば,

$$Q_1(x) \stackrel{\mathrm{def}}{=} x-1, \quad Q_2(x) \stackrel{\mathrm{def}}{=} x-2, \quad P(x)=1$$

とすると,

$$\mathrm{ord}_0(Q_1(x)) \;=\; \mathrm{ord}_0(Q_2(x)) \;=\; \mathrm{ord}_0(P(x)) \;=\; 0$$

であるが,

$$\mathrm{ord}_0(Q_1(x)+P(x)) \;=\; \mathrm{ord}_0(x) = \;1\; \neq \;0\; =\; \mathrm{ord}_0(x-1) \;=\; \mathrm{ord}_0(Q_2(x)+P(x))$$

となる.

- $Q(x),\, P(x) \in \mathcal{O}_a^{=1}$ (あるいは $\mathcal{O}_a^{\times}$, あるいは $\mathcal{O}_a^{\triangleright}$) であっても, $Q(x)+P(x) \in \mathcal{O}_a^{=1}$ (あるいは $\mathcal{O}_a^{\times}$, あるいは $\mathcal{O}_a^{\triangleright}$) とは限らない. 実際, 例えば,

$$Q(x) \;\stackrel{\mathrm{def}}{=}\; x+1, \quad P(x) \;\stackrel{\mathrm{def}}{=}\; 1, \quad R(x) \;\stackrel{\mathrm{def}}{=}\; -x-1$$

とすると, $Q(x),\, P(x) \in \mathcal{O}_0^{=1}$ であるが, $Q(x)+P(x) \notin \mathcal{O}_0^{=1}$ となる. また, $Q(x),\, R(x) \in \mathcal{O}_0^{\times}$ (従って $\in \mathcal{O}_0^{\triangleright}$) であるが, $Q(x)+R(x) \notin \mathcal{O}_0^{\triangleright}$ (従って $\notin \mathcal{O}_0^{\times}$) となる.

このように,

> $\mathrm{ord}_a(Q(x)+P(x))$ を $\mathrm{ord}_a(Q(x))$ と $\mathrm{ord}_a(P(x))$ のみから計算することはできない

となっており, また,

> $\mathcal{O}_a^{=1},\, \mathcal{O}_a^{\times},\, \mathcal{O}_a^{\triangleright}$ のいずれに対しても, その中では自由には加法ができない

となっています.

こういった事実から,

> $\mathrm{ord}_a,\, \mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ は, 乗法との相性は良いが, 加法との相性は良くない,

あるいは,

> $\mathrm{ord}_a,\, \mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ は, 加法的な概念ではなく乗法的な概念である

と考えることは, 少なからず妥当なことだと言えると思います.

ちなみに, 時間の都合でここでは詳しい議論は与えられませんが, 上の議論の結論同様, §1 の後半で定義を与えた $\mathbb{Q}$ の 2 つの部分集合

$$\mathbb{Z}_{(p)}^{=1} \;\subseteq\; \mathbb{Z}_{(p)}^{\triangleright} \;\subseteq\; \mathbb{Q}$$

に対しても, (例えば “その中で自由に乗法はできるが加法はできない” という観点から) やはり “乗法との相性は良いが, 加法との相性は良くない”, あるいは, “加法的な概念ではなく乗法的な概念である” と考えることができます.

3　主定理とその証明の準備

本講義の目標は, 以下の主張の内容, 及び, その証明を理解していただくことです.

主定理

集合 $\mathbb{C}(x)$ と $\mathbb{P}^1$ が与えられたとき,

(1)　$\mathbb{C}(x)$ の乗法構造

$$\begin{array}{ccc} \mathbb{C}(x)\times\mathbb{C}(x) & \longrightarrow & \mathbb{C}(x) \\ (Q(x),P(x)) & \mapsto & Q(x)\cdot P(x), \end{array}$$

(2)　$\mathbb{P}^1$ の元で添字付けられた $\mathbb{C}(x)$ の部分集合の族

$$\left\{\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x)\right\}_{a\in\mathbb{P}^1}$$

という情報から, $\mathbb{C}(x)$ の加法構造

$$\begin{array}{ccc} \mathbb{C}(x)\times\mathbb{C}(x) & \longrightarrow & \mathbb{C}(x) \\ (Q(x),P(x)) & \mapsto & Q(x)+P(x) \end{array}$$

を記述する手続きが存在する.

この定理は, 大雑把に言えば, (抽象的な) 集合 $\mathbb{C}(x)$ が与えられたとき,

- $\mathbb{C}(x)$ の掛け算,　- $\mathbb{C}(x)$ の部分集合の族 $\left\{\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x)\right\}_{a\in\mathbb{P}^1}$

を入力すると,

$\mathbb{C}(x)$ の足し算

がその出力として得られるあるアルゴリズムが存在する, ということを主張しています. ここで, この講義の観点から着目していただきたい点は,

このアルゴリズムの入力側の情報は, どれも乗法的な情報である

という点です. “$\mathbb{C}(x)$ の掛け算” は乗法そのものですので, 文字どおり “乗法的な情報” ですし, また, “部分集合 $\mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x)$” が (加法的でなく) 乗法的な概念である, という事実は, §2 の後半で観察したとおりです. つまり, 上の定理の内容を更に大雑把にまとめるならば,

$\mathbb{C}(x)$ のある乗法的な情報から, その加法を復元するある手続きが存在する

となります.

上の定理の証明は §4 で与えられます. そのために, この §3 では, いくつかの補題を準備します. まず最初の補題 3.1 は簡単に確認できると思います.

補題 3.1. $Q(x) \in \mathbb{C}(x)$ を有理式とする.

(i)　以下の 2 条件は同値.

(1)　$Q(x) = 0$.

(2)　任意の有理式 $P(x) \in \mathbb{C}(x)$ に対して, $Q(x) \cdot P(x) = Q(x)$.

(ii)　以下の 2 条件は同値.

(1)　$Q(x) = 1$.

(2)　任意の有理式 $P(x) \in \mathbb{C}(x)$ に対して, $Q(x) \cdot P(x) = P(x)$.

(iii)　以下の 2 条件は同値.

(1)　$Q(x) = -1$.

(2)　$Q(x) \neq 1$ かつ $Q(x)^2 = 1$.

次の補題 3.2 もそれほど難しい内容ではないので, その証明は省略します. 演習問題として考えてみてください.

補題 3.2. 0 でない有理式 $Q(x) \in \mathbb{C}(x)$ に対して, 以下の 2 条件は同値.

(1)　$Q(x)$ は複素数, 即ち, $Q(x) \in \mathbb{C}$ $(\subseteq \mathbb{C}(x))$.

(2)　任意の $a \in \mathbb{P}^1$ に対して, $\mathrm{ord}_a(Q(x)) = 0$.

次の補題 3.3 もそれほど難しくないので, その証明は演習問題とさせていただきます.

補題 3.3. 0 でない有理式 $Q(x)$, $P(x) \in \mathbb{C}(x)$ に対して, 以下の 2 条件は同値.

(1)　$Q(x) = P(x)$.

(2)　$Q(x)$, $P(x) \in \mathcal{O}_a^{\triangleright}$ なる無限に多くの $a \in \mathbb{P}^1$ に対して, $Q(a) = P(a)$.

次の補題 3.4 は少々ややこしい格好をしていますが, 実質的な内容はそれほど難しくないと思います.

補題 3.4. a, b, $c \in \mathbb{P}^1$ を相異なる $\mathbb{P}^1$ の元; $s \in \mathbb{C}$ を 0 でない複素数とする. このとき, 以下の 2 つの条件 $(1)_s^{(a,b,c)}$, $(2)_s^{(a,b,c)}$ を満たす 0 でない有理式 $Q_s^{(a,b,c)}(x)$ が唯一つ存在する.

$(1)_s^{(a,b,c)}$　$\mathrm{ord}_a(Q_s^{(a,b,c)}(x)) = -1, \quad \mathrm{ord}_b(Q_s^{(a,b,c)}(x)) = 1, \quad \mathrm{ord}_z(Q_s^{(a,b,c)}(x)) = 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a, b\})$.

$(2)_s^{(a,b,c)}$　$Q_s^{(a,b,c)}(c) = s$.

$\infty \notin \{a, b, c\}$ の場合の補題 3.4 を証明しましょう. (a, b, c のどれかが ∞ の場合の証明は, 演習問題とさせていただきます.) $\infty \notin \{a, b, c\}$ の場合, 所望の $Q_s^{(a,b,c)}(x)$ は以下の有理式です.

$$Q_s^{(a,b,c)}(x) \stackrel{\mathrm{def}}{=} s \cdot \frac{c-a}{c-b} \cdot \frac{x-b}{x-a} \in \mathbb{C}(x).$$

この有理式が補題の主張の中の 2 つの条件 $(1)_s^{(a,b,c)}$, $(2)_s^{(a,b,c)}$ を満たすことは簡単に確認できます. 最後に, 補題の主張の中の 2 つの条件 $(1)_s^{(a,b,c)}$, $(2)_s^{(a,b,c)}$ を満たす有理式がこれしかないことを確認しましょう. もしもある有理式 $Q(x)$ が条件 $(1)_s^{(a,b,c)}$ を満たすとしますと, 簡単に確認できるように, ある 0 でない複素数 $t \in \mathbb{C}$ が存在して,

$$Q(x) \ = \ t \cdot \frac{x-b}{x-a}$$

と書けます. $t \cdot \dfrac{c-b}{c-a} = Q(c)$ ですので, 更に $Q(x)$ が条件 $(2)_s^{(a,b,c)}$ を満たすとしますと, $s = t \cdot \dfrac{c-b}{c-a}$ となり, 特に, $Q(x) = Q_s^{(a,b,c)}(x)$ となります. これで補題 3.4 の証明は終了です.

次は補題 3.5 です. 記号の複雑度が段々と上がっていますが, やはり, 実質的な内容はそれほど難しくないと思います.

補題 3.5. a, b, c, $d \in \mathbb{P}^1$ を相異なる $\mathbb{P}^1$ の元; s, $t \in \mathbb{C}$ を 0 でない複素数とする. このとき, 以下の 2 つの条件 $(1)_{(s,t)}^{(a,b,c,d)}$, $(2)_{(s,t)}^{(a,b,c,d)}$ を満たす 0 でない有理式 $Q_{(s,t)}^{(a,b,c,d)}(x)$ が唯一つ存在する.

$(1)_{(s,t)}^{(a,b,c,d)}$　$\mathrm{ord}_a(Q_{(s,t)}^{(a,b,c,d)}(x)) \geq -1$, $\mathrm{ord}_z(Q_{(s,t)}^{(a,b,c,d)}(x)) \geq 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a\})$.

$(2)_{(s,t)}^{(a,b,c,d)}$　$Q_{(s,t)}^{(a,b,c,d)}(b) = Q_t^{(a,d,c)}(b)$, $Q_{(s,t)}^{(a,b,c,d)}(d) = Q_s^{(a,b,c)}(d)$　(有理式 $Q_t^{(a,d,c)}(x)$, $Q_s^{(a,b,c)}(x)$ については, 補題 3.4 を参照).

補題 3.5 を証明しましょう. 補題 3.4 の証明と同様, 先に “答え” を書いてしまいますと, 所望の $Q_{(s,t)}^{(a,b,c,d)}(x)$ は以下の有理式で与えられます.

$$Q_{(s,t)}^{(a,b,c,d)}(x) \ \stackrel{\mathrm{def}}{=} \ Q_s^{(a,b,c)}(x) + Q_t^{(a,d,c)}(x) \ \in \ \mathbb{C}(x).$$

この有理式が補題の主張の中の 2 つの条件 $(1)_{(s,t)}^{(a,b,c,d)}$, $(2)_{(s,t)}^{(a,b,c,d)}$ を満たすこと, 特に 0 でないこと, は簡単に確認できます. 最後に, 補題の主張の中の 2 つの条件 $(1)_{(s,t)}^{(a,b,c,d)}$, $(2)_{(s,t)}^{(a,b,c,d)}$ を満たす有理式がこれしかないことを確認しましょう. この事実を確認するために, ある有理式 $Q(x)$ が条件 $(1)_{(s,t)}^{(a,b,c,d)}$, $(2)_{(s,t)}^{(a,b,c,d)}$ を満たし, かつ,

$$P(x) \ \stackrel{\mathrm{def}}{=} \ Q(x) - Q_s^{(a,b,c)}(x) - Q_t^{(a,d,c)}(x) \ \neq \ 0$$

となると仮定して, 矛盾を導きましょう. $Q(x)$ が条件 $(1)_{(s,t)}^{(a,b,c,d)}$ を, $Q_s^{(a,b,c)}(x)$ が条件 $(1)_s^{(a,b,c)}$ を, $Q_t^{(a,d,c)}(x)$ が条件 $(1)_t^{(a,d,c)}$ をそれぞれ満たすことから,

(I)　$\mathrm{ord}_a(P(x)) \geq -1, \quad \mathrm{ord}_z(P(x)) \geq 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a\})$

となることが, それほどの困難なく確かめられます. 次に $Q(x)$ が条件 $(1)_{(s,t)}^{(a,b,c,d)}$ と $(2)_{(s,t)}^{(a,b,c,d)}$ を, $Q_s^{(a,b,c)}(x)$ が条件 $(1)_s^{(a,b,c)}$ と $(2)_s^{(a,b,c)}$ を, $Q_t^{(a,d,c)}(x)$ が条件 $(1)_t^{(a,d,c)}$ と $(2)_t^{(a,d,c)}$ をそれぞれ満たすことから,

$$P(b) \ = \ Q(b) - Q_s^{(a,b,c)}(b) - Q_t^{(a,d,c)}(b) \ = \ Q_t^{(a,d,c)}(b) - 0 - Q_t^{(a,d,c)}(b) \ = \ 0,$$

$$P(d) \ = \ Q(d) - Q_s^{(a,b,c)}(d) - Q_t^{(a,d,c)}(d) \ = \ Q_s^{(a,b,c)}(d) - Q_s^{(a,b,c)}(d) - 0 \ = \ 0$$

となることが, つまり, b と d が有理式 $P(x)$ の零点であることが確かめられます. これは

(II)　$\mathrm{ord}_b(P(x)) \geq 1$, $\mathrm{ord}_d(P(x)) \geq 1$

という条件と同値であることを思い出しましょう. 従って, (I) と (II) によって,

$$\sum_{z\in\mathbb{P}^1}\mathrm{ord}_z(P(x)) \;=\; \mathrm{ord}_a(P(x))+\mathrm{ord}_b(P(x))+\mathrm{ord}_d(P(x))+\sum_{z\in\mathbb{P}^1\setminus\{a,b,d\}}\mathrm{ord}_z(P(x)) \;\geq\; -1+1+1+0=1$$

となり, 命題 2.9 の後半部分の等式に矛盾します. これで補題 3.5 の証明が完了しました.

次に, 以下の補題を確認しましょう.

補題 3.6. 補題 3.5 で得られた有理式 $Q_{(s,t)}^{(a,b,c,d)}(x)\in\mathbb{C}(x)$ は, 等式

$$Q_{(s,t)}^{(a,b,c,d)}(c) \;=\; s+t$$

を満たす.

実際, 補題 3.5 の証明から,

$$Q_{(s,t)}^{(a,b,c,d)}(x) \;=\; Q_s^{(a,b,c)}(x)+Q_t^{(a,d,c)}(x)$$

であることを知っていますので, $Q_s^{(a,b,c)}(x)$, $Q_t^{(a,d,c)}(x)$ が条件 $(2)_s^{(a,b,c)}$, $(2)_t^{(a,d,c)}$ をそれぞれ満たすことから,

$$Q_{(s,t)}^{(a,b,c,d)}(c) \;=\; Q_s^{(a,b,c)}(c)+Q_t^{(a,d,c)}(c) \;=s+t$$

となり, 結論が従います.

§3 の最後に, $\mathcal{O}_a^{\triangleright}$ という部分集合と代入という操作に関する以下の補題を確認しましょう.

補題 3.7. $a\in\mathbb{P}^1$ とする.

(i)　0 でない有理式 $Q(x)\in\mathbb{C}(x)$ に対して, 以下の条件は同値.

(1)　$\mathrm{ord}_a(Q(x))=1$.

(2)　$\mathcal{O}_a^{\triangleright}$ の任意の元は, $\mathcal{O}_a^{\times}$ の元と $Q(x)$ の非負の巾 (つまり, $Q(x)^n$, ただし, n は非負整数) の積で表される.

(ii)　$Q(x)\in\mathcal{O}_a^{\triangleright}$ に対して, $Q(x)$ に a を代入して得られる複素数 $Q(a)\in\mathbb{C}$ は, 以下の 2 つの条件のいずれかを満たす唯一つの複素数 $s\in\mathbb{C}$ である.

(1)　$s=0$ かつ $\mathrm{ord}_a(Q(x))\neq 0$.

(2)　$s\cdot Q(x)^{-1}\in\mathcal{O}_a^{=1}$.

まず最初に (i) を証明しましょう. (1) $\Rightarrow$ (2) を証明するために, $\mathrm{ord}_a(Q(x))=1$ を仮定して, また, $\mathcal{O}_a^{\triangleright}$ の任意の元 $P(x)\in\mathcal{O}_a^{\triangleright}$ をとります. このとき, $\mathcal{O}_a^{\triangleright}$ の定義から, $n\overset{\mathrm{def}}{=}\mathrm{ord}_a(P(x))\geq 0$ となります. また, 命題 2.10, (i), より,

$$\mathrm{ord}_a\big(P(x)\cdot Q(x)^{-n}\big) \;=\; \mathrm{ord}_a(P(x))+(-n)\cdot\mathrm{ord}_a(Q(x)) \;=\; n+(-n)\cdot 1=0$$

ですので, $\mathcal{O}_a^{\times}$ の定義から, $R(x)\overset{\mathrm{def}}{=}P(x)\cdot Q(x)^{-n}\in\mathcal{O}_a^{\times}$ となります. 一方,

$$P(x) \;=\; P(x)\cdot Q(x)^{-n}\cdot Q(x)^n \;=\; R(x)\cdot Q(x)^n$$

ですので, 条件 (2) の成立が確認できました. 次に, (2) ⇒ (1) を証明するために, 条件 (2) が成立することを仮定しましょう. $a \neq \infty$ の場合, $\mathrm{ord}_a(x-a) = 1$, 特に, $x - a \in \mathcal{O}_a^{\triangleright}$ ですので, 条件 (2) から, $\mathcal{O}_a^{\times}$ のある元 $P(x) \in \mathcal{O}_a^{\times}$ と正整数 n が存在して,

$$x - a \ = \ P(x) \cdot Q(x)^n$$

と書けるはずです. この等式の両辺の "ord_a" を 命題 2.10, (i), を用いて計算してみましょう. すると

$$1 \ = \ \mathrm{ord}_a(x-a) \ = \ \mathrm{ord}_a\big(P(x)\cdot Q(x)^n\big) \ = \ \mathrm{ord}_a(P(x))+n\cdot\mathrm{ord}_a(Q(x)) \ = \ 0+n\cdot\mathrm{ord}_a(Q(x)) \ = \ n\cdot\mathrm{ord}_a(Q(x))$$

となります. その定義から $\mathrm{ord}_a(Q(x))$ は整数ですので, 正整数である n と整数である $\mathrm{ord}_a(Q(x))$ を掛けて 1 とするためには, $n = \mathrm{ord}_a(Q(x)) = 1$ でなければなりません. 特に, 条件 (1) の成立が確認されました. $a = \infty$ の場合には, 上と同様の議論を, "$x - a$" の代わりに $\dfrac{1}{x}$ を用いて実行することにより, 条件 (1) の成立が確認されます.

最後に補題 3.7, (ii), を証明しましょう. まず $Q(a) \in \mathbb{C}$ が, 補題の主張内の 2 つの条件のいずれかを満たすことを確認します. もしも $Q(a) = 0$ ならば, a は $Q(x)$ の零点ですから, 特に, $\mathrm{ord}_a(Q(x)) \neq 0$ が従い, 条件 (1) が成立します. 次に $Q(a) \neq 0$ と仮定しましょう. この場合, a は $Q(x)$ の零点でも極でもありませんので, $Q(x) \in \mathcal{O}_a^{\times}$ となります. また, $Q(a) \in \mathbb{C}$ より $\mathrm{ord}_a(Q(a)) = 0$, つまり, $Q(a) \in \mathcal{O}_a^{\times}$ となります. 従って, 命題 2.10, (iii), より $Q(a) \cdot Q(x)^{-1} \in \mathcal{O}_a^{\times} \subseteq \mathcal{O}_a^{\triangleright}$ となり, $Q(a) \cdot Q(x)^{-1}$ に a を代入することが可能だということがわかります. さて, 実際に代入してみましょう. 有理式 $Q(a) \cdot Q(x)$ に a を代入してみますと, $Q(a) \cdot Q(a)^{-1} = 1$ となります. ですので, $\mathcal{O}_a^{=1}$ の定義から, $Q(a) \cdot Q(x)^{-1} \in \mathcal{O}_a^{=1}$ が得られ, 特に, 条件 (2) の成立が確認されます.

次に, 補題 3.7, (ii), の主張内の 2 つの条件のいずれかを満足する複素数が $Q(a) \in \mathbb{C}$ のみである, という主張を確認しましょう. もしも複素数 $s \in \mathbb{C}$ が条件 (1) を満足すると仮定しますと, $Q(x) \in \mathcal{O}_a^{\triangleright}$ (つまり, $\mathrm{ord}_a(Q(x)) \geq 0$) という仮定と条件 (1) の後半部分から, $\mathrm{ord}_a(Q(x)) > 0$ が得られます. これは, a が $Q(x)$ の零点であるということを意味していますので, 特に, $Q(a) = 0$ となり, 条件 (1) の前半部分から, $Q(a) = 0 = s$ という所望の結論が得られます. 次に, 複素数 $s \in \mathbb{C}$ が条件 (2) を満足したと仮定しましょう. すると, $\mathcal{O}_a^{=1}$ の定義から, 有理式 $s \cdot Q(x)^{-1}$ に a を代入して得られる値が 1 となります. さて, 実際に代入してみましょう. 有理式 $s \cdot Q(x)^{-1}$ に a を代入してみますと, $s \cdot Q(a)^{-1}$ $(= 1)$ となります. ですので, $s = Q(a)$ という所望の結論が得られます.

4 加法構造の復元の手続き

本講義の主定理の内容を復習しましょう.

主定理

集合 $\mathbb{C}(x)$ と $\mathbb{P}^1$ が与えられたとき,

(1) $\mathbb{C}(x)$ の乗法構造

$$\begin{array}{ccc} \mathbb{C}(x) \times \mathbb{C}(x) & \longrightarrow & \mathbb{C}(x) \\ (Q(x), P(x)) & \mapsto & Q(x) \cdot P(x), \end{array}$$

(2) $\mathbb{P}^1$ の元で添字付けられた $\mathbb{C}(x)$ の部分集合の族

$$\left\{ \mathcal{O}_a^{=1} \subseteq \mathcal{O}_a^{\triangleright} \subseteq \mathbb{C}(x) \right\}_{a \in \mathbb{P}^1}$$

という情報から, $\mathbb{C}(x)$ の加法構造

$$\begin{array}{ccc} \mathbb{C}(x) \times \mathbb{C}(x) & \longrightarrow & \mathbb{C}(x) \\ (Q(x), P(x)) & \mapsto & Q(x) + P(x) \end{array}$$

を記述する手続きが存在する.

この §4 では, 上の主張を証明します. 所望の手続きを, 以下のとおり, 7 つのステップにわけました.

手続き 1 (0, 1, -1):

(i) 以下の条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を 0 と書く: 任意の $\mathbb{C}(x)$ の元 $P(x) \in \mathbb{C}(x)$ に対して, $Q(x) \cdot P(x) = Q(x)$.

(ii) 以下の条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を 1 と書く: 任意の $\mathbb{C}(x)$ の元 $P(x) \in \mathbb{C}(x)$ に対して, $Q(x) \cdot P(x) = P(x)$.

(iii) 以下の条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を -1 と書く: $Q(x) \neq 1$ ((ii) を参照) かつ $Q(x) \cdot Q(x) = 1$ ((ii) を参照).

この手続きによって定められた “0”, “1”, “-1” が, 皆さんの知っている “0”, “1”, “-1” と一致していることは, 補題 3.1 から直ちに従います.

手続き 2 ($Q(x)^{-1}$):
0 でない (手続き 1, (i), を参照) $\mathbb{C}(x)$ の元 $Q(x) \in \mathbb{C}(x)$ に対して, 以下の条件を満たす $\mathbb{C}(x)$ の唯一つの元 $P(x) \in \mathbb{C}(x)$ を $Q(x)^{-1}$ と書く: $Q(x) \cdot P(x) = 1$ (手続き 1, (ii), を参照).

この手続きによって定められた “$Q(x)^{-1}$” が, 皆さんの知っている “$Q(x)^{-1}$” と一致していることは, 簡単に確認できると思います.

手続き 3 (ord_a):
$a \in \mathbb{P}^1$, $n \in \mathbb{Z}$ とする. また, $Q(x) \in \mathbb{C}(x)$ を 0 でない (手続き 1, (i), を参照) $\mathbb{C}(x)$ の元とする.

(i) 以下の条件が成立するとき, $\mathrm{ord}_a(Q(x)) = 0$ と書く: $Q(x) \in \mathcal{O}_a^{\triangleright}$ かつ $Q(x)^{-1} \in \mathcal{O}_a^{\triangleright}$ (手続き 2 を参照).

(ii) $\mathbb{C}(x)$ の部分集合 $\mathcal{O}_a^{\times} \subseteq \mathbb{C}(x)$ を以下のように定める:

$$\mathcal{O}_a^{\times} \stackrel{\mathrm{def}}{=} \{\, Q(x) \in \mathbb{C}(x) \,|\, Q(x) \neq 0 \,\text{かつ}\, \mathrm{ord}_a(Q(x)) = 0 \,\}$$

((i), 及び, 手続き 1, (i), を参照.)

(iii) 以下の条件が成立するとき, $\mathrm{ord}_a(Q(x)) = 1$ と書く: $\mathcal{O}_a^{\triangleright}$ の任意の元は, $\mathcal{O}_a^{\times}$ ((ii) を参照) の元と $Q(x)$ の非負の巾 (つまり, $\overbrace{Q(x)\cdots Q(x)}^{d}$, ただし, d は非負整数) の積で表される.

(iv) 以下の条件が成立するとき, $\mathrm{ord}_a(Q(x)) = n$ と書く:

(1) $n = 0$ ならば, (i) のとおり.

(2) $n = 1$ ならば, (iii) のとおり.

(3) $n \geq 2$ ならば, ある元 $P(x) \in \mathbb{C}(x)$ が存在して, $\mathrm{ord}_a(P(x)) = 1$ ((iii) を参照) かつ $Q(x)^{-1} \cdot \overbrace{P(x)\cdots P(x)}^{n} \in \mathcal{O}_a^{\times}$ ((ii), 及び, 手続き 2 を参照) が成立.

(4) $n \leq -1$ ならば, ある元 $P(x) \in \mathbb{C}(x)$ が存在して, $\mathrm{ord}_a(P(x)) = 1$ ((iii) を参照) かつ $Q(x) \cdot \overbrace{P(x)\cdots P(x)}^{-n} \in \mathcal{O}_a^{\times}$ ((ii) を参照) が成立.

手続き 3, (i), によって定められた "$\mathrm{ord}_a(Q(x)) = 0$" が定義 2.4 や定義 2.8, (i), で定義された "$\mathrm{ord}_a(Q(x)) = 0$" と一致していることは, $\mathcal{O}_a^{\triangleright}$ の定義と命題 2.10, (i), から従います. 手続き 3, (ii), によって定められた "$\mathcal{O}_a^{\times} \subseteq \mathbb{C}(x)$" が定義 2.6 や定義 2.8, (ii), で定義された "$\mathcal{O}_a^{\times} \subseteq \mathbb{C}(x)$" と一致することは簡単に確認できると思います. 手続き 3, (iii), によって定められた "$\mathrm{ord}_a(Q(x)) = 1$" が定義 2.4 や定義 2.8, (i), で定義された "$\mathrm{ord}_a(Q(x)) = 1$" と一致していることは, 補題 3.7, (i), から従います. 手続き 3, (iv), によって定められた "$\mathrm{ord}_a(Q(x)) = n$" が定義 2.4 や定義 2.8, (i), で定義された "$\mathrm{ord}_a(Q(x)) = n$" と一致していることは, 命題 2.10, (i), と ord_a の値が 1 であるような有理式の存在 ($a \neq \infty$ ならば, 例えば $x - a$; $a = \infty$ ならば, 例えば $\frac{1}{x}$) から従います.

手続き 4 ($\mathbb{C}$):
$\mathbb{C}(x)$ の部分集合 $\mathbb{C} \subseteq \mathbb{C}(x)$ を以下のように定義する:

$$\mathbb{C} \stackrel{\mathrm{def}}{=} \{0\} \cup \Big(\bigcap_{a \in \mathbb{P}^1} \mathcal{O}_a^{\times}\Big) \subseteq \mathbb{C}(x)$$

(手続き 1, (i), 及び, 手続き 3, (ii), を参照).

この手続きによって定められた “$\mathbb{C} \subseteq \mathbb{C}(x)$” が, 従来の “$\mathbb{C} \subseteq \mathbb{C}(x)$” と一致していることは, 補題 3.2 から従います.

手続き 5 (代入):
$a \in \mathbb{P}^1$, $Q(x) \in \mathcal{O}_a^{\triangleright}$, $s \in \mathbb{C} \subseteq \mathbb{C}(x)$ (手続き 4 を参照) に対して, 以下の 2 つの条件のいずれかが成立するとき, $Q(a) = s$ と書く:

(1)　$s = 0$ (手続き 1, (i), を参照) かつ $\mathrm{ord}_a(Q(x)) \neq 0$ (手続き 3, (i), を参照).

(2)　$s \cdot Q(x)^{-1} \in \mathcal{O}_a^{=1}$ (手続き 2 を参照).

この手続きによって定められた “$Q(a) = s$” が, 従来の “$Q(a) = s$” と一致していることは, 補題 3.7, (ii), から従います.

手続き 6 ($\mathbb{C}$ の加法構造):
$s, t \in \mathbb{C} \subseteq \mathbb{C}(x)$ (手続き 4 を参照) に対して, 以下の条件を満たす $\mathbb{C} \subseteq \mathbb{C}(x)$ の唯一つの元 $u \in \mathbb{C}$ を $s + t$ と書く:

(1)　$s = 0$ (手続き 1, (i), を参照) ならば, $u = t$.

(2)　$t = 0$ (手続き 1, (i), を参照) ならば, $u = s$.

(3)　$0 \notin \{s, t\}$ (手続き 1, (i), を参照) の場合, まず最初に, 相異なる $\mathbb{P}^1$ の元 a, b, c, d を固定する. 以下の 2 つの条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を $Q_s^{(a,b,c)}(x)$ と書く:

- $\mathrm{ord}_a(Q(x)) = -1$, $\mathrm{ord}_b(Q(x)) = 1$, $\mathrm{ord}_z(Q(x)) = 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a, b\})$ (手続き 3, (iv), を参照).
- $Q(c) = s$ (手続き 5 を参照).

また, 以下の 2 つの条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を $Q_t^{(a,d,c)}(x)$ と書く:

- $\mathrm{ord}_a(Q(x)) = -1$, $\mathrm{ord}_d(Q(x)) = 1$, $\mathrm{ord}_z(Q(x)) = 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a, d\})$ (手続き 3, (iv), を参照).
- $Q(c) = t$ (手続き 5 を参照).

次に, 以下の 2 つの条件を満たす $\mathbb{C}(x)$ の唯一つの元 $Q(x) \in \mathbb{C}(x)$ を $Q_{(s,t)}^{(a,b,c,d)}(x)$ と書く:

- $\mathrm{ord}_a(Q(x)) \geq -1$, $\mathrm{ord}_z(Q(x)) \geq 0 \quad (\forall z \in \mathbb{P}^1 \setminus \{a\})$ (手続き 3, (iv), を参照).
- $Q(b) = Q_t^{(a,d,c)}(b)$, $Q(d) = Q_s^{(a,b,c)}(d)$ (手続き 5 を参照).

このとき, $u = Q_{(s,t)}^{(a,b,c,d)}(c)$ (手続き 5 を参照) が成立.

この手続きの正当性は補題 3.4 と補題 3.5 が保証して, また, この手続きで定められた “$s + t$” が, 皆さんの知っている “$s + t$” と一致していることは, 補題 3.6 から従います.

手続き 7 ($\mathbb{C}(x)$ の加法構造):
$Q(x)$, $P(x) \in \mathbb{C}(x)$ に対して, 以下の条件を満たす $\mathbb{C}(x)$ の唯一つの元 $R(x) \in \mathbb{C}(x)$ を $Q(x) + P(x)$ と書く:

(1) $Q(x) = (-1) \cdot P(x)$ (手続き 1, (iii), を参照) ならば, $R(x) = 0$.

(2) $Q(x) = 0$ (手続き 1, (i), を参照) ならば, $R(x) = P(x)$.

(3) $P(x) = 0$ (手続き 1, (i), を参照) ならば, $R(x) = Q(x)$.

(4) $Q(x) \neq (-1) \cdot P(x)$ (手続き 1, (iii), を参照) かつ $0 \notin \{Q(x), P(x)\}$ (手続き 1, (i), を参照) ならば, $Q(x)$, $P(x)$, $R(x) \in \mathcal{O}_a^{\triangleright}$ となるようなすべての $a \in \mathbb{P}^1$ に対して, $Q(a) + P(a) = R(a)$ (手続き 5, 及び, 手続き 6 を参照) が成立.

この手続きで定められた "$Q(x) + P(x)$" が, 皆さんの知っている "$Q(x) + P(x)$" と一致していることは, 命題 2.9 の前半部分と補題 3.3 から従います.

以上のステップにより, $\mathbb{C}(x)$ の加法構造の復元が完了しました.

参考文献

[1] Y. Hoshi, On the field-theoreticity of homomorphisms between the multiplicative groups of number fields, to appear in *Publ. Res. Inst. Math. Sci.*

[2] S. Mochizuki, *Topics in Absolute Anabelian Geometry III: Global Reconstruction Algorithms*, RIMS Preprint **1626** (March 2008).

[3] M. Saïdi and A. Tamagawa, A prime-to-p version of Grothendieck's anabelian conjecture for hyperbolic curves over finite fields of characteristic $p > 0$, *Publ. Res. Inst. Math. Sci.* **45** (2009), no. **1**, 135-186.

[4] M. Saïdi and A. Tamagawa, On the Hom-form of Grothendieck's birational anabelian conjecture in positive characteristic, *Algebra Number Theory* **5** (2011), no. **2**, 131-184.

[5] A. Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), no. **2**, 135-194.

[6] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.* (**2**) **106** (1977), no. **3**, 589-598.