編者緒言

本書は，藤原松三郎著「代数学」第一巻および第二巻を現代仮名遣いに改め，術語の一部を現在ひろく用いられているものに置き換えたものである．

本書の第一巻は 1928 年に，第二巻は 1929 年に刊行されたが，それは二十世紀の代数学の教科書のスタイルを根本的に変えた van der Waerden の “Moderne Algebra” が出版される直前であった（同書第 I 巻は 1930 年，第 II 巻は 1931 年の刊行）．また，我が国において代数学の古典として読み継がれてきた高木貞治による「初等整数論講義」および「代数学講義」はそれぞれ 1930 年，31 年に出版されている．今日の目で眺めたとき，これらのことが本書をその組立てにおいて，また，内容において極めて独自なものとしている．

本書の特徴として，代数学全般にわたり基礎的理論を詳述し，かつ高度な内容にまで説き及んでいるだけでなく，概念導入にあたりその背景を説明し具体例を挙げるなど丁寧な叙述をしているため，自修書としても適していると言えよう．さらに，第八章および第九章で系統的に論じられている Fourier の定理，Sturm の定理あるいは Routh–Hurwitz の定理など代数方程式の根の分布に関する理論や Newton 法や Horner 法などの近似解法は，現代の大学の学部教育で教えられることは稀であるが，力学系理論，物理学や工学等において重要であり，これらの方面の専門家にとっても貴重な参考書となっている．また，原著は巻末に補遺を追加して，本文の訂正や文献の追加を行っている．特に，最後に加えられた補遺は，江戸時代に和算家が得た諸結果を本巻で展開されている西洋数学の成果と対比したもので，著者が心血を注いだ和算史研究の成果の一端を知ることができる．本改訂版では「和算家による独創的成果」と題を改めて収録した．

術語については，著者が独語，英語等から直接訳出したものも相当数あると思われる．そのため，第二巻序言でも述べられているように，他書とは異なる術語が散見され，その中には定着しなかったものもある．本改訂版では，「方列」を「行列」とするなど，それらを現在標準的に用いられているものに置き換えた．しかしながら，著者の

意図を尊重して，変更しなかったものや，敢えて広く流通しているとは言い難いものに置き換えた場合もあることをお断りしておく．例えば，原著では「整函数」は，「多項式」（「整式」とも言う）を指しているが，数論における整数と有理数に対応するものとして，整函数と有理函数と呼ぶことには充分な正当性があると考える．しかし現在では，専ら複素平面上で正則な関数を整関数と呼んでいるのを考慮して，本改訂版では原著にもある「有理整関数」を採用することとした．

編者らの浅学非才のため，思わぬ誤解から却って原著の明晰性を損ねてはいないかと恐れる．読者の叱正を俟って改訂をしていく所存である．

改訂にあたり術語や文献についてご教示いただいた都築暢夫東北大学教授に感謝の意を表したい．

2019 年 1 月

編著者

第２巻 編者緒言

本書は，藤原松三郎著「代数学」第二巻を現代仮名遣いに改め，術語の一部を現在ひろく用いられているものに置き換えたものである．

原著第二巻初版が出版されたのは 1929 年であった．以来九十年の間に代数学は大きく発展し，かつ変貌を遂げた．就中，二十世紀中葉までに数学の抽象化が著しく進行し，数学の叙述の仕方にも大きな影響を及ぼした．しかし，抽象化を推進した人々は二十世紀初頭までに蓄積された近代数学の成果を熟知していたことを忘れてはならない．本書では代数学と数論について講じられているが，著者は巻末の「結語」において，数論とは数の個性に関する学問であり，代数学とは要素間に加減乗除の四則演算（もしくはその一部）が許される集合の形式を論ずる学問であると総括している．つまり，近代的代数学とは，数のもつ性質を抽象して構築されたものである．同時に，群論，環論，体論という代数学の核となる理論が一旦確立されると，数の個性についてもこれらの理論的枠組みの中で論じられていくことになる．本書第一巻で展開された数と代数方程式に関する古典的理論を踏まえて，第二巻では，代数方程式の代数的可解性についてのガロアの理論など近代的代数学の中心的話題を丁寧に講述する．代数的可解性とは，加減乗除の四則演算と冪根をとる操作を有限回行って得られる数の性質であるから，数論の問題でもある．ここに数の個性を抽象的枠組みの中で論じる必然性が生まれる．代数的整数の理論を述べた第 16 章では「イデアル」が導入された経緯を詳細に説くことから始まっている．さながら，近代代数学の建築過程を目撃する思いである．本書が優れた自修書として位置付けられる所以である．

術語については，著者が独語，英語等から直接訳出したものも相当数あると思われる．そのため，本巻序言でも述べられているように，他書とは異なる術語が散見され，その中には定着しなかったものもある．本改訂版では，「方列」を「行列」とするなど，それらを現在標準的に用いられているものに置き換えた．しかしながら，著者の意図を尊重して，変更しなかったものや敢えて広く流通しているとは言い難いものに置き換えた場合もあることをお断りしておく．例えば，原著では「整函数」は，「多項式」

(「整式」とも言う) を指しているが，数論における整数と有理数に対応するものとして，整函数と有理函数と呼ぶことには充分な正当性があると考える．しかし現在では専ら，複素平面上で正則な関数を整関数と呼ぶのを考慮して，本改訂版では原著にもある「有理整関数」を採用することとした．

また，代数学の発展の過程で，例えば「同型」のように術語の意味が変わってきたものもあれば，「不変部分群」のように基本語であるにもかかわらず用いられなくなってきたものもある．これらは現代的な群論をすでに学んだ読者にとっては却って理解を妨げることにもなりかねないため，改訂にあたり現代的な用語に置き換えるとともに，解説のための一節を設けることにした．

編者らの浅学非才のため，思わぬ誤解から却って原著の明晰性を損ねてはいないかと恐れる．読者の叱正を俟って改訂をしていく所存である．

改訂にあたり術語や文献についてご教示いただいた都築暢夫東北大学教授に感謝の意を表したい．

2020 年 1 月

編著者

第10章　群　　論[†]

第1節　群と部分群

10.1. **群の定義.**　本章は群の一般性質を論ずることを目的とする．我々はすでに第 1 巻，§1.30 において群の定義を述べたことがあるが，念のためここにこれを繰返そう．

今 a, b, c, ... なる元よりなる集合 G を考える．これらの元は我々の思惟の対象となり得るものならば，数，演算，変換等，何でもよろしい．

G の任意の二元 a, b の間にはある一定の結合関係が規定されたとし，これを積の形 ab で表そう．この G が次の性質をもつ場合に，G は一つの**群**を作ると定義する．

(1) G の任意の二元 a, b の結合 ab がまた G の元である．

(2) 結合法則 $a(bc) = (ab)c$ が成立する．

(3) G のいかなる元 a に対しても $ae = ea = a$ を満足するような元 e が唯一つ存在する．これを**単位元**と名づける．

(4) G の任意の元 a に対し，$aa' = a'a = e$ を満足する元 a' が唯一つ存在する．これを a の**逆元**と名づけ，a^{-1} を以て表す．

これから直ちに次のことが分かる．

$$(ab)^{-1} = b^{-1}a^{-1}.$$

$$ax = b \quad \text{ならば} \quad x = a^{-1}b.$$

$$xa = b \quad \text{ならば} \quad x = ba^{-1}.$$

[†] 本章に関しては Burnside, Theory of groups of finite order, 2.ed., 1911; Miller–Blichfeldt–Dickson, Finite group, 1915; Speiser, Die Theorie der Gruppen von endlichen Ordnung, 2. Aufl., 1927; 園博士，高等代数学上巻，1928; 竹内博士，群論初歩（輓近高等数学講座），1928 参照．文献に関しては，Miller, Report on recent progress in the theory of groups of finite order, Bull. American Math. Soc. (2) 5, 7, 9, 14, 1898–1908 参照．

有限個の元よりなる群を**有限群**，無限個よりなるものを**無限群**と名づける．本章では専ら有限群について論ずるから，単に群といえば，特に断らない限り，有限群を意味する．

例えば，四個の数字 1, 2, 3, 4 から作られる，あらゆる置換（§7.2）を元とする集合を考え，二つの置換の結合関係として置換の積をとる．二つの置換の積はまた一つの置換であって，単位置換，逆置換がそれぞれ単位元，逆元に相当するから，この集合は明らかに群を作る．置換を元とする群を**置換群**と名づける[*1]．

一般群論の発展はこの置換群の研究から出発したのである．

群の他の一例として，一点のまわりの回転を元とする集合をとる．角 θ_1, θ_2 の回転を結合したものを角 $\theta_1 + \theta_2$ の回転と考えれば，あらゆる角の回転の集合は明らかに一つの無限群を作る．単位元は角 0 の回転であり，角 θ の回転の逆元は角 $-\theta$ の回転である．もし回転角が π/n の倍数なるもののみを元とすれば，有限群が得られる．

10.2. 群の定義の単純化. 上述の群の定義は，ウェーバーの定義をピアポントが簡単にした形であるが，さらにこれを次の形になし得ることは，ムーア，ディクスン，ハンティントン[*1]によって示された．

(1) G の任意の二元 a, b の結合として，第三元 $c = ab$ が唯一通りに定まる．

(2) $a(bc) = (ab)c$.

(3) 少なくとも一つの元 e が存在し，任意の元 a に対し，$ae = a$ が成立する．

(4) 任意の元 a に対し，$aa' = e$ に適合する a' が少なくとも一つ存在する[*2]．

これから単位元は唯一つ存在すること，並びに a の逆元もまた唯一つ存在することが，次のように証明される．

(A) 任意の a に対し $ae = a$ ならば，$ea = a$ となる．かつ $aa' = e$ ならば $a'a = e$ である．

これを証明すると，(4) によれば，a' に対して $a'a'' = e$ なる a'' が少なくとも一つ存在する．よって

$$a = ae = a(a'a'') = (aa')a'' = ea''.$$

§10.1,*1 〔**編者注**：詳しくは §10.25 で述べる．〕

§10.2,*1 E. H. Moore, Dickson, Huntington, Trans. American Math. Soc. 3, 1902; 5, 1904; 6, 1905.

*2 〔**編者注**：まず (3) で存在が保証される e を一つ固定すれば，任意の元 a をとるとき，それに応じて a' が定まり $aa' = e$ が成立する．つまり，a' は a と e を指定して初めて定まる．〕

第11章　ガロアの方程式論[†]

第1節　代数的数体

11.1. **数体と部分数体.**　我々は本章において，ガロアが創めた，群論を基礎とする方程式の理論を述べよう．そのために，まず代数的数体の概念からはじめる．

我々はすでに第 1 巻，§1.31 において，体の一般の定義を与えた．ここに再録して読者の記憶を新たにしよう．

有限個または無限個の元（要素）からなる一つの集合 $\mathfrak{K}$ を考え，その任意の二元 A, B の間に二種の異なる結合 $A+B$, $A\cdot B$ が次の I–IV で規定された場合に，$\mathfrak{K}$ は一つの**体**[*1]をなすという．

I. $\mathfrak{K}$ は $A+B$ なる結合に関して群をなす．その単位元を E_0 とする．

II. $\mathfrak{K}$ より E_0 を除いた集合が，$A\cdot B$ なる結合に対して群をなす．その単位元を E_1 とする．

III. $\mathfrak{K}$ においては分配法則

$$A\cdot(B+C)=A\cdot B+A\cdot C,\qquad (B+C)\cdot A=B\cdot A+C\cdot A$$

が成立する．

IV. $\mathfrak{K}$ においては交換法則

$$A+B=B+A,\qquad A\cdot B=B\cdot A$$

が成立する．

0 のみからなる集合は，本書では，これを除外する．

例えば 0 のみからなる集合は一つの体をなす．

[†] 本章に関しては H. Weber, Lehrbuch der Algebra 1, または Kleines, Lehrbuch der Algebra, 1912; Fricke, Lehrbuch der Algebra 1, 1924 参照.

§11.1,*1　体の一般研究に関しては Steinitz, Journ. f. Math. 137, 1910 参照.

素数 p を法としてすべての整数を互いに合同なる類 $C_0, C_1, C_2, \ldots, C_{p-1}$ に分類し，これらの類を元と考えれば，この p 個の元は明らかに一つの体をなす．これは一つの**有限体**である．

我々はすでに第 1 巻，§1.31, §3.7, §5.2 において，すべての有理数，すべての実数，すべての複素数からなる集合はそれぞれ有理数体，実数体，複素数体を作ることを証明した．これらは無限の元よりなる数体である．

一般に，数の集合 $\mathfrak{K}$ において，$\mathfrak{K}$ に属する任意の二数の和，差，積および商がまた $\mathfrak{K}$ に属する場合，すなわち加減乗除の四則が零による除法を除いて $\mathfrak{K}$ 内で無制限に許される場合には，$\mathfrak{K}$ は明らかに一つの**数体**をなす．

任意の数体 $\mathfrak{K}$ は必ず 0 でない数 a を含むから，$\mathfrak{K}$ はまた $a/a = 1$ を含む．

従って有理数体が $\mathfrak{K}$ に含まれる．

このように数体の元の一部分が一つの数体を作れば，後者を前者の**部分数体**と名づけ，前者を後者の**包括数体**という．

よって次の定理が成立する．

定理．　有理数体はあらゆる数体の部分数体である．

数体 $\mathfrak{K}$ に属しない一数 α をとり，$\mathfrak{K}$ の数と α とに加減乗除の四則を有限回施して得られる数の全体は，また一つの新しい数体をなす．これを $\mathfrak{K}(\alpha)$ で表し，$\mathfrak{K}$ に α を**添加**した数体という．$\mathfrak{K}(\alpha)$ の数は明らかに $\mathfrak{K}$ の数を係数にもつ α の有理関数の形に表される．

数 α の代わりに変数 x を $\mathfrak{K}$ に添加すれば，$\mathfrak{K}$ の数を係数にもつ x の有理関数の体，すなわち**有理関数体** $\mathfrak{K}(x)$ が得られる．$\mathfrak{K}(x)$ に属する有理整関数[*2]，有理関数をそれぞれ $\mathfrak{K}$ **の有理整関数**，$\mathfrak{K}$ **の有理関数**という．$f(x)$ が $\mathfrak{K}$ の有理整関数ならば，方程式 $f(x) = 0$ を $\mathfrak{K}$ **の方程式**という．

11.2.　既約有理整関数と既約方程式．　数体 $\mathfrak{K}$ に属する有理整関数 $f(x)$ が，同じく $\mathfrak{K}$ に属する二つの有理整関数の積の形に表され得ない場合に，$f(x)$ は数体 $\mathfrak{K}$ において**既約**であるという．既約の反対を**可約**という (§6.18)．

既約なる概念はその根底におかれた数体を離れては不定である．数体 $\mathfrak{K}$ において既約であっても，$\mathfrak{K}$ のある包括数体においては必ずしも既約ではない．

[*2] 〔**編者注**：**多項式**ともいう．〕

第12章　行列の理論[†]

第1節　行　　列

12.1. **行列の四則.**　我々は §7.6 ですでに行列なる語に遭遇した．ここでは行列の演算に関する法則を述べよう[*1].

n^2 個の数 a_{ik} $(i,k=1,2,\dots,n)$ を正方形に配列したものを n **次の行列** (matrix) と名づけ，これを

$$A=\begin{Vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{Vmatrix}, \quad \text{または} \quad \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

で表す．あるいは簡単に $A=(a_{ik})$ で表すことにする．a_{ik} を行列 A の (i,k) **要素**と名づける．

この要素が作る行列式 $|a_{ik}|$ を**行列の行列式**と名づけ，$|A|$ で表す．

我々は行列を支配する法則を次のように規定する．

相等.　行列 $A=(a_{ik})$, $B=(b_{ik})$ は $a_{ik}=b_{ik}$ $(i,k=1,2,\dots,n)$ なるときに限り**相等**しいと定義し，これを $A=B$ で表す．

---

† 本章に関しては Muth, Theorie und Anwendung der Elementarteiler, 1899; Dickson, Modern algebraic theories, 1926; Bromwich, Quadratic forms and their classifications by means of invariant factors, 1906 (Cambridge Tracts 3) 参照.

行列 (matrix) は Cayley (Phil. Trans., 1858, Collected Math. Papers 2, p.475) が初めて論じ，彼と独立に少し遅れて Laguerre (Journ. l'École polyt. Cah. 42, 1867, Oeuvres 1, p.221) が論じた．以下論ずる記号的方法は主として Frobenius (Journ. f. Math. 84, 1878) が創始したのである.

§12.1, *1 〔**編者注**：本章では断りがない限り常に正方行列のみを扱う．原著では方列という語が用いられている.〕

すべての要素が 0 なる行列を**零行列**といい，単に O で表すことにする．

和． 行列 $A=(a_{ik})$, $B=(b_{ik})$ の**和**として $(a_{ik}+b_{ik})$ をとる．これを $A+B$ で表す．加法の交換法則，結合法則の成立することはいうまでもない．

差． $(a_{ik}-b_{ik})$ によって A, B の**差**と定義し，これを $A-B$ で表す．

積． $A=(a_{ik})$, $B=(b_{ik})$ の**積**は

$$c_{ik}=a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{in}b_{nk}$$

を要素とする行列 $C=(c_{ik})$ と定義する．これを AB で表す．

AB の行列式は $|AB|=|A|\cdot|B|$ に等しい (§7.12)．

t を任意の数とし，$t\,a_{ik}$ を要素とする行列を tA で表す．tA の行列式 $|tA|$ は $t^n|A|$ に等しい．これは対角要素が t に等しく，その他の要素は 0 に等しい行列と A との積にほかならない．

ここに注意すべきは，**行列に対しては乗法の交換法則が必ずしも成立しない**ことである．これは

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix}=\begin{bmatrix}2&1\\1&1\end{bmatrix},\qquad \begin{bmatrix}1&0\\1&1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}$$

が一致しないことを見れば明らかである．

それでは乗法の結合法則はどうであろうか．

$A=(a_{ik})$, $B=(b_{ik})$, $C=(c_{ik})$ とし，$A(BC)$, $(AB)C$ の (i,k) 要素を計算すれば，それぞれ

$$\sum_j a_{ij}\left(b_{j1}c_{1k}+b_{j2}c_{2k}+\cdots+b_{jn}c_{nk}\right),$$

$$\sum_j \left(a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}\right)c_{jk}$$

となり互いに相等しい．故に乗法の結合法則は成立する．

分配法則もまた成立する．

何となれば $A(B+C)$ の (i,k) 要素は

$$a_{i1}(b_{1k}+c_{1k})+a_{i2}(b_{2k}+c_{2k})+\cdots+a_{in}(b_{nk}+c_{nk})$$

$$=(a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{in}b_{nk})+(a_{i1}c_{1k}+a_{i2}c_{2k}+\cdots+a_{in}c_{nk})$$

第 13 章　二元二次形式の数論[†]

第 1 節　整係数の二次形式

13.1.　二次形式の数論上の問題.　二変数 $x,\ y$ の二次形式

$$f = ax^2 + bxy + cy^2 \tag{1}$$

を二元二次形式と名づけ，$a,\ b,\ c$ をその第一，第二，第三の係数と呼ぶ．ここではしばらく係数を実数に限ることにする．

与えられた整数 m がいかなる条件の下に二つの整数の平方の和に表すことができるか，換言すれば

$$x^2 + y^2 = m$$

を満たす整数 $(x,\ y)$ がいかなる場合に存在するかという問題は，すでにギリシャでディオファンタスの算術書に現れている．これを拡張すれば

$$ax^2 + bxy + cy^2 = m$$

を整数 $x,\ y$ で解く問題が生ずる．これはオイラー，ラグランジュ，ルジャンドル等の十八世紀末の学者によって論じられた．

ガウス[*1]に至っては，この問題はむしろ従となり，二次形式 (1) の組織的研究が主となった．ガウスの研究は徹底的ではあるが，すこぶる複雑である．これに対してディリクレ[*2]は二次無理数および複素数の概念を利用して，大いに理論を簡明にした．次にそれを示そう．

二次形式 (1) はその係数さえ与えればそれで定まるから，これを $(a,\ b,\ c)$ で表そ

[†]　本章に関しては，Dirichlet, Vorlesungen über Zahlentheorie 4 Aufl., 1894; Cahen, Théorie des nombres 2, 1924. 文献については Dickson, History of the theory of numbers 3, 1923 参照.

§13.1,*1　Gauss, Disquisitiones Arith., §153–307, Werke 1, pp.120–379.

*2　Dirichlet, Berliner Abh., 1854, Werke 2, p.139.

う[*3]．二次形式論においては主要な位置を占めるものは判別式

$$D = b^2 - 4ac$$

である[*4]．ここでは D は 0 とならず，また整数の平方とならないものと仮定しておく．

二次形式 (1) に一次変換

$$S: \quad \begin{cases} x = \alpha x' + \beta y', \\ y = \gamma x' + \delta y' \end{cases} \qquad (\alpha,\ \beta,\ \gamma,\ \delta \text{ は整数};\ \alpha\delta - \beta\gamma = \pm 1) \tag{2}$$

を施せば

$$f' = a'x'^2 + b'x'y' + c'y'^2 \tag{3}$$

の形に変わる．係数 a'，b'，c' は

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned} \tag{4}$$

を満たす．

この関係を

$$(a', b', c') = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} (a, b, c)$$

で表そう．(4) を書換えて

$$\begin{aligned} 2a' &= \alpha(2a\alpha + b\gamma) + \gamma(b\alpha + 2c\gamma), \\ b' &= \beta(2a\alpha + b\gamma) + \delta(b\alpha + 2c\gamma) \\ &= \alpha(2a\beta + b\delta) + \gamma(b\beta + 2c\delta), \\ 2c' &= \beta(2a\beta + b\delta) + \delta(b\beta + 2c\delta). \end{aligned}$$

従って

$$b'^2 - 4a'c' = (b^2 - 4ac)(\alpha\delta - \beta\gamma)^2 = b^2 - 4ac. \tag{5}$$

[*3] ガウスは二次形式を $ax^2 + 2bxy + cy^2$ と書いて，これを (a, b, c) で表した．このガウス流の二次形式の理論では，公式が本書のものと違うことに注意せねばならない．

[*4] ガウスは D を Determinant と呼んだ．今でもそれにならう学者がある．また人によると D を二次形式の行列式，$-D$ を判別式という．

第14章　一次変換群

第1節　多面体群[†]

14.1.　一次変換群と射影変換群.　一次変換を元とする群を**一次変換群**と名づける．これは行列を元とする群とも見られる．

例えば

$$s_1:\quad x_1{}' = x_1,\ x_2{}' = x_2; \qquad s_2:\quad x_1{}' = x_2,\ x_2{}' = x_1;$$
$$s_3:\quad x_1{}' = \varepsilon x_1,\ x_2{}' = \varepsilon^2 x_2; \qquad s_4:\quad x_1{}' = \varepsilon^2 x_2,\ x_2{}' = \varepsilon x_1; \quad (\varepsilon^3 = 1)$$
$$s_5:\quad x_1{}' = \varepsilon^2 x_1,\ x_2{}' = \varepsilon x_2; \qquad s_6:\quad x_1{}' = \varepsilon x_2,\ x_2{}' = \varepsilon^2 x_1,$$

およびこれに対応する行列

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ \begin{bmatrix}\varepsilon & 0\\ 0 & \varepsilon^2\end{bmatrix},\ \begin{bmatrix}0 & \varepsilon^2\\ \varepsilon & 0\end{bmatrix},\ \begin{bmatrix}\varepsilon^2 & 0\\ 0 & \varepsilon\end{bmatrix},\ \begin{bmatrix}0 & \varepsilon\\ \varepsilon^2 & 0\end{bmatrix}$$

は三次対称群と同型な群を作る．

二つの一次変換

$$s:\qquad x_1{}' = ax_1 + bx_2, \quad x_2{}' = cx_1 + dx_2;$$
$$t:\qquad x_1{}' = a'x_1 + b'x_2, \quad x_2{}' = c'x_1 + d'x_2$$

の係数が

$$a' = ka,\ \ b' = kb,\ \ c' = kc,\ \ d' = kd$$

を満たす場合

$$\kappa = \begin{bmatrix}k & 0\\ 0 & k\end{bmatrix}; \qquad x_1{}' = kx_1,\ \ x_2{}' = kx_2$$

[†]　第 1 節に関しては Weber, Algebra 2; Fricke, Algebra 2, 1926; Miller–Blichfeldt–Dickson, Finite Group, 1915 参照．文献に関しては Wiman, Enzyklopädie der Math. Wiss. I 参照．

とおけば

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix},$$

すなわち

$$t = \kappa s = s \kappa$$

となる．この場合に，t は s と同一の**射影変換**

$$x' = (ax + b)/(cx + d)$$

を表すという．κ の形のものを**等比変換**と名づける．

以上に述べたことは，n 変数の一次変換についても同様である．

一つの一次変換群 G の元のうちに，同一の射影変換を表すものが存在する場合と，存在しない場合とがある．

s, t が同一の射影変換を表せば，t は s と等比変換 κ との積であるから，G に含まれる等比変換の全体を $s_1,\ s_2,\ \ldots,\ s_h$ とすれば，それだけで G の一つの部分群 H を作る．G を H で分解したものを

$$G = H + Ht_1 + Ht_2 + \cdots + Ht_{\nu-1}$$

とすれば，剰余類 Ht_i の元は

$$s_1 t_i,\ s_2 t_i,\ \ldots,\ s_h t_i$$

である．これらは明らかに t_i と同一の射影変換を表す．

逆に t_i と同一の射影変換を表す任意の元を τ とすれば，$\tau {t_i}^{-1}$ は等比変換であるから，$s_1,\ s_2,\ \ldots,\ s_h$ のいずれかの一つとならねばならない．これを s_k とすれば，$\tau = s_k t_i$ となって Ht_i に含まれる．

故に Ht_i は t_i と同一の射影変換を表す G の元の全体である．

等比変換は他の元と可換であるから，H は G の正規部分群である．

一次変換

$$s: \quad x_i = a_{i1} {x_1}' + a_{i2} {x_2}' + \cdots + a_{in} {x_n}', \qquad (i = 1, 2, \ldots, n)$$

において

$$x_1/x_n = y_1, \quad x_2/x_n = y_2, \quad \ldots, \quad x_{n-1}/x_n = y_{n-1},$$

第15章　不変式論†

第1節　二次形式の不変式

15.1.　変換群と不変式.　これまで我々はしばしば不変式なる概念に遭遇した．有限一次変換群の不変式に対しては §14.2, §14.10 で論じた．

この不変式の概念は有限群に限らず，これを無限群に拡張することができる．

例えば二変数の一次変換

$$x_1 = \alpha x_1' + \beta x_2', \qquad x_2 = \gamma x_1' + \delta x_2', \qquad (\alpha\delta - \beta\gamma \neq 0)$$

において係数 $\alpha,\ \beta,\ \gamma,\ \delta$ は任意の数を表すものと考えれば，その全体は明らかに一つの無限群 G を作る．

この一次変換を二元二次形式

$$f(x_1,\ x_2) = a_0\, {x_1}^2 + 2a_1\, x_1 x_2 + a_2 {x_2}^2$$

に施せば，$f(x_1,\ x_2)$ は次のように変わり

$$f'(x_1',\ x_2') = a_0'\, {x_1'}^2 + 2a_1' x_1' x_2' + a_2'\, {x_2'}^2$$

となる．ただし

$$\begin{aligned} a_0' &= \alpha^2\, a_0 + 2\alpha\gamma\, a_1 + \gamma^2\, a_2, \\ a_1' &= \alpha\beta\, a_0 + (\alpha\delta + \beta\gamma)\, a_1 + \gamma\delta\, a_2, \\ a_2' &= \beta^2\, a_0 + 2\beta\delta\, a_1 + \delta^2\, a_2. \end{aligned}$$

これは $(a_0,\ a_1,\ a_2)$ を $(a_0',\ a_1',\ a_2')$ に移す一次変換である．すなわち群 G の一

† 本章に関しては Weitzenböck, Invariantentheorie, 1923; Gordan, Vorlesungen über Invariantentheorie 2, 1887; Grace-Young, The algebra of Invariants, 1903 参照．文献については F. Meyer, Bericht über den gegenwärtigen Stand der Invariantentheorie, Jahresber. D.M.V. 1, 1892 参照．

つの元に $(a_0,\ a_1,\ a_2)$ の一つの変換が対応する．従って後者もまた一つの群 H を作る．これを G **によって誘導された群**と名づける．H は G と同型である．然るに $(a_0,\ a_1,\ a_2),\ (a_0',\ a_1',\ a_2')$ の間には

$$a_1'^2 - a_0'a_2' = (\alpha\delta - \beta\gamma)^2(a_1^2 - a_0a_2)$$

なる関係が成立する (§13.1)．故に判別式 $a_1^2 - a_0a_2$ は明らかに H の一つの不変式である．

H の不変式を**二元形式** $f(x_1,\ x_2)$ **の不変式**と名づける．

この事実はすでにガウスの認めた所であるが，ブール[*1]はこれを n 元 m 次形式に拡張してその判別式の不変性を示した．それから出発して二元形式の不変式論を始めたのは，ケイリー[*2]である．

本節では主として二元形式の不変式について論じよう．

15.2. 二元形式の不変式．

二元 n 次形式

$$f(x_1,\ x_2) = a_0x_1^n + \binom{n}{1}a_1x_1^{n-1}x_2 + \binom{n}{2}a_2x_1^{n-2}x_2^2 + \cdots + a_nx_2^n \qquad (1)$$

に一次変換

$$x_1 = \alpha\, y_1 + \beta\, y_2, \qquad x_2 = \gamma\, y_1 + \delta\, y_2 \qquad (2)$$

を施したものを

$$g(y_1,\ y_2) = b_0y_1^n + \binom{n}{1}b_1y_1^{n-1}y_2 + \binom{n}{2}b_2y_1^{n-2}y_2^2 + \cdots + b_ny_2^n \qquad (3)$$

とする．

$f(x_1,\ x_2)$ の係数 $a_0,\ a_1,\ \ldots,\ a_n$ の関数 $J(a_0,\ a_1,\ \ldots,\ a_n)$ が

$$J(b_0,\ b_1,\ \ldots,\ b_n) = \rho\, J(a_0,\ a_1,\ \ldots,\ a_n) \qquad (4)$$

なる関係を満足する場合，$J(a_0,\ a_1,\ \ldots,\ a_n)$ を**二元形式** $f(x_1,\ x_2)$ **の不変式**と名づける．ただし ρ は $f(x_1,\ x_2)$ の係数に無関係で，唯変換 (2) の係数 $(\alpha,\ \beta,\ \gamma,\ \delta)$ のみのある関数を表すものとする．

---

§15.1,*1 Boole, Cambridge Math. J. 4, 1845.

*2 Cayley, Cambridge Math. J. 4, 1845; Cambridge and Dublin Math. J. 1, 1846, Collected Math. Papers 1, pp.80–112．これらは Journ. f. Math. 10, 1846 にまとめられている．

第16章　代数数体の数論†

第1節　代数的整数

16.1. **代数数体の数論の発達.**　有理数体の数論を一般の代数数体に拡張するのはガウス[*1]に始まる.

$x^4 \equiv D \pmod m$ に適合する整数 x が存在する場合に，D を m の四次剰余という．平方剰余の場合 (§2.17) と同様に，四次剰余の理論を建設せんがために，ガウスは初めて有理数体 $\mathfrak{R}$ に $i=\sqrt{-1}$ を添加した数体 $\mathfrak{R}(i)$ における数論を論じた．これについでヤコビおよびアイゼンシュタインは $\mathfrak{R}$ に 1 の立方根 $\rho=(-1+\sqrt{-3})/2$ を添加した数体 $\mathfrak{R}(\rho)$ の数論を論じた．然るにクンマーはフェルマーの最後定理 (§2.38) を $\mathfrak{R}(e^{2\pi i/p})$ の数論の助けをかりて証明できたと信じ，これをディリクレに示したとき，ディリクレの答は次のものであった．曰く「数体 $\mathfrak{R}(e^{2\pi i/p})$ においても $\mathfrak{R}$ におけると同様に，素因数分解がただ一通りに可能なることが証明されない以上は，この証明は完全でない」と．クンマーはこのディリクレの注意によって研究を進めた結果，素因数分解の一意性は必ずしも常に成立するとは限らないことを発見した．彼はこの困難を切り抜けるために，新たに理想数 (ideale Zahlen) なる概念を導入した[*2].

ついでデデキントはクンマー[*3]の理想数に代えて，イデアル (Ideal) なる概念を以

† 本章に関しては Hecke, Theorie der algebraischen Zahlen, 1923; Landau, Einführung in die elementare und analytischen Theorie der algebraischen Zahlen und der Ideale, 1918; Hilbert, Bericht über die Theorie der algebraischen Zahlkörper, Jahresber. d. D.M.V. 4, 1897 参照．1897 年までの文献は Hilbert, Bericht に詳しい．1898 年以後の文献については Dickson, Mitchell, Vandiver, Wahlin, Report on algebraic numbers, Bull. National Research Council 5, 1923.

§16.1,*1 Gauss, Comm. soc. sci. Gottingensis 7, 1832, Werke 2, pp.95–148.

*2 Kummer, Journ. f. Math. 35, 1847.

*3 Dedekind, Dirichlet's Vorlesungen über Zahlentheorie 2. Aufl., 1871, Suppl. X. 4. Aufl., 1894, Suppl. XI で多少改良された.

てし，現今のイデアル論の基礎を築いた．クロネッカー[*4]もまたデデキントとは独立に代数数体の数論を建設した．

我々は本章において，デデキントのイデアル論の大要を述べることにする．このためにまず代数的整数について論ずることにしよう．

16.2. 代数的整数. 我々は §11.4 において，有理数体 $\mathfrak{R}$ における n 次既約方程式

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0, \quad (a_k \text{ は有理整数}) \tag{1}$$

の根として n 次の代数的整数を定義した．この定義から直ちに次のことが証明される (§11.4).

(I) α, β が代数的整数ならば，$\alpha+\beta, \alpha-\beta, \alpha\beta$ もまた代数的整数である．

(II) 代数的整数 α が有理数ならば，α は有理整数である．

(III) 代数的整数 α の共役数はまた代数的整数である．

逆に (I), (II), (III) に適合する数 α の共役数を $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ とすれば，$(\alpha, \alpha_1, \ldots, \alpha_{n-1})$ の基本対称関数は (I), (III) によって代数的整数である．従って (II) によって有理整数となるから，α は (1) の形の方程式の根となる．

代数的整数 α, β, γ が $\alpha = \beta\gamma$ に適合すれば，α は β で**整除**されるという．α を β の**倍数**，β を α の**約数**または**因数**と名づける．

$\mathfrak{R}$ における方程式

$$g(x) = x^m + b_1 x^{m-1} + \cdots + b_{m-1}x + b_m = 0, \quad (b_k \text{ は有理整数}) \tag{2}$$

の根は $g(x)$ が既約でない場合でも代数的整数を表す．

何となれば，ガウスの定理 (§6.19) によって，(2) の左辺は (1) の左辺の形の既約因子に分解されるからである．

$\alpha_0, \alpha_1, \ldots, \alpha_n$ を任意の代数的整数とすれば

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1}x + \alpha_n = 0 \tag{3}$$

の根 ξ はまた代数的数であって，$\alpha_0 = 1$ ならば，ξ は代数的整数を表す (§11.4). $\alpha_0 \neq 1$ の場合でも次の定理が成立する．

[*4] Kronecker, Journ. f. Math. 92, 1882, Werke 2, p.245.

第17章　超　越　数

第1節　リューヴィル超越数

17.1.　代数的数の必要条件.　我々はすでに代数的数の性質を論じ，代数的数でない数を**超越数**と定義した (§11.3)．しかし超越数なるものが果たして存在するか否か．これが第一に決定せねばならない問題である．

このために我々はまず代数的数の必要条件を調べよう．その条件に適合しないものがあれば，これは当然超越数でなければならない．

n 次の代数的数 ω が実数である場合には次の定理が成立する．

定理.　**n 次の代数的数 ω が実数ならば，有限数 M が定まり，有理整数 p/q をいかに選んでも**

$$|\omega - p/q| > M/q^n$$

が成立する[*1]**.**

ω が適合する有理整係数の既約方程式を

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

とする．

δ を一定にして $\omega - \delta$, $\omega + \delta$ の間にある任意の有理数 p/q をとれば，微分学における平均値定理によって

$$f(p/q) = f(\omega + p/q - \omega) = f(\omega) + (p/q - \omega)f'(\xi)$$

に適合する実数 ξ が $\omega - \delta$, $\omega + \delta$ 内で定められる．ただし $f'(x)$ は $f(x)$ の導関数を表すものとする．

$f(\omega) = 0$ であるから

---

§17.1,*1　Liouville, Comptes Rendus 18, 1844; Journ. de Math. (1) 16, 1851.

$$f(p/q) = (p/q - \omega)f'(\xi)$$

となる．然るに $\omega - \delta \leqq x \leqq \omega + \delta$ に適合するすべての実数 x に対し $|f'(x)|$ は有限の最大値をもつ．これを K とすれば，K はもちろん p/q に無関係に定まる．一方では

$$f(p/q) = (a_0p^n + a_1p^{n-1}q + \cdots + a_nq^n)/q^n$$

の分子を A とすれば 0 とはならない．何となれば，有理数 p/q が $f(x) = 0$ の根となれば，$f(x)$ は $\mathfrak{R}$ で可約となるからである．従って A は 0 でない整数であるから $|A| \geqq 1$ となる．

よって $f(p/q) = (p/q - \omega)f'(\xi)$ から

$$K|p/q - \omega| \geqq 1/q^n, \text{ すなわち } |p/q - \omega| \geqq 1/Kq^n$$

が得られる．

有理数 p/q が $(\omega - \delta, \omega + \delta)$ の外にあれば $|p/q - \omega| \geqq \delta$ である．故に M を δ, $1/K$ のいずれよりも小さくとれば，p/q をいかに選んでも

$$|\omega - p/q| > M/q^n$$

が成立する．

この簡単な事実から直ちに次の定理が得られる．

定理．　正整数 n および実数 M をいかに選んでも

$$|\omega - p/q| \leqq M/q^n$$

に適合する有理数 p/q が存在すれば，ω は超越数である．

この条件に適合する超越数を**リューヴィル超越数**と名づけよう．このような数が実際無限に存在することは次の例で明らかである．

小数で表された

$$\omega = \frac{a_1}{10^{k_1}} + \frac{a_2}{10^{k_2}} + \cdots + \frac{a_n}{10^{k_n}} + \cdots$$

なる数を考える．ただし $a_1, a_2, \ldots, a_n, \ldots$ の各々は 0, 1, 2, …, 9 のいずれか一つを表すものとする．

$$k_n = \nu_1\nu_2\cdots\nu_n, \quad \nu_1 < \nu_2 < \cdots < \nu_n \to \infty, \quad (\nu_i \text{ は整数})$$

と仮定すれば，ω は一つのリューヴィル超越数を表す．