代数拡大の系譜（平成１８年）

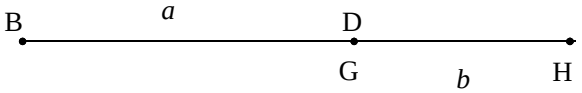
1. 作図可能な数

(1) 四則演算と開平の作図

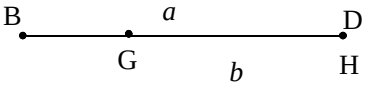
デカルト Renè Descartes (1596~1650)は, 彼の著書「方法序説」の別冊「幾何学」の中で, 次のように記している.「線分の間の四つないし五つの代数的演算（加法,減法, 乗法, 除法, 根の抽出）を定義し, それらの演算のいかなる結果も線分として解釈できる 」と.

（注）古代ギリシャ時代より, 作図は定規とコンパスで描くことになっている.

1) 同一直線上で, 和や差を線分で考えている.

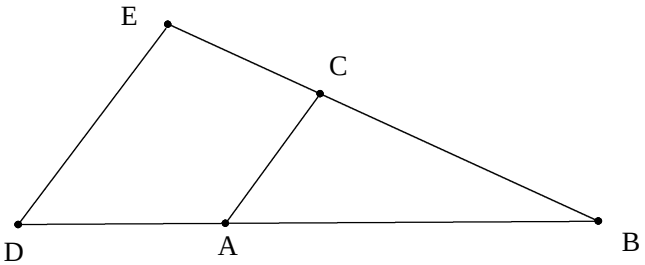


$a + b$ = BH



$a - b$ = BG　($a > b$)

2) 同一直線上に, AB = e (単位の長さ), DB = a　となるようにとる. B を通る直線上に　BC = b,　BE = c　となるようにとる. D を通り, AC に平行に DE を引くと,

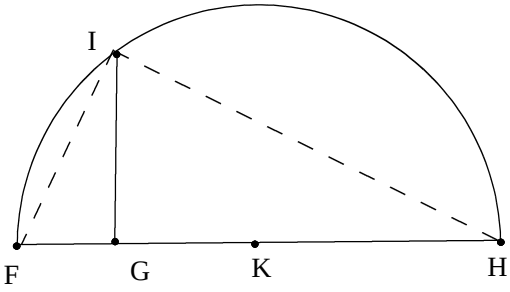


△ABC ∽ △DBE　だから

CB : BE = AB : DB

∴ BE = $a \times b$,　CB = $\dfrac{c}{a}$

3) 直線上に, FG = e (単位の長さ), GH = a となるようにとる. FH の中点を K とし, K を中心に FH を直径とする半円を描く. G を通り, FH に垂線を立て, 半円との交点を I とする.



△FGI ∽△IGH　だから

FG : GI = GI : GH

∴ GI = $\sqrt{a}$

このようにして, 四則演算と開平で出来る数は定規とコンパスで描くことが出来ることを示している.

2. 代数的数と代数拡大

古代ギリシャ以来，作図は定規とコンパスのみで行うことになっている．こうした制約を設けることで，古代ギリシャ人は次の難問に直面した．

(1) 与えられた角を三等分することは出来ない．（角の三等分問題）

(2) 与えられた立方体の体積の二倍に等しい立方体は作図出来ない．（立方体の倍積問題）

(3) 与えられた円の面積に等しい正方形は，作図出来ない．（円積問題）

こうした難問を解決するために，人々は悪戦苦闘し数学を発展させてきた．

1) 定規とコンパスによる作図

定規とコンパスで作図することは，次のように解釈されている．まず平面に点集合 S　　が与えられ，次の操作を有限回繰り返すことである．

(1) S 上の二点を結ぶ直線が定規で描くことができる．

(2) S 上の点を中心として，与えられた長さを半径とする円が，コンパスで描くことができる．

(3) 二直線の交点を S に加える．

(4) 直線と円の交点を S に加える．

(5) 二円の交点を S に加える．

(3)について，直線 AB, CD の交点は，四点 A, B, C, D の座標から四則演算で求めることができる．

(4)について，直線 AB と円 P の交点は，A,B の座標と円 P の中心の座標および半径の長さ r から四則演算と開平で求めることができる．

(5)について，二円の差をとることによって(4)に帰着される．

このように，作図は与えられた実数から四則演算と開平お操作を有限回繰り返して，新しい実数を求めることである．そこで，作図可能な数を次のように定義する．

定　義　有理係数の多項式

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

の根になる数を「代数的数」という．

（注）作図可能な数は代数的数であるが，逆は成り立たない．（例）　$\sqrt[3]{a}$

定　理　a, b　が代数的数ならば，$a + b$,　$a - b$, ab, $\dfrac{a}{b}$　$(b \neq 0)$ も代数的数である．

証　明　a, b　を根とする有利係数多項式 $f(x)$, $g(x)$ をとる．

$$f(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n, \quad g(x) = x^m + q_1 x^{m-1} + \cdots + q_{m-1} x + q_m$$

a, b　が代数的数だから $f(a) = 0$,　$g(b) = 0$

$a^n + p_1 a^{n-1} + \cdots + p_{n-1} a + p_n = 0, \quad b^m + q_1 b^{m-1} + \cdots + q_{m-1} b + q_m = 0$

$\therefore \quad a^n = -(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n \quad (n-1 \text{ 次}),$

$b^m = -(q_1 b^{m-1} + \cdots + q_{m-1} b + q_m \quad (m-1 \text{ 次})$

$\therefore \ a^{-1} = -p_n^{-1}(a^{n-1} + p_1 a^{n-2} + \cdots + p_{n-1}) \quad (n-1 \text{ 次}),$

$b^{-1} = -q_m^{-1}(b^{m-1} + q_1 b^{m-2} + \cdots + q_{m-1}) \quad (m-1 \text{ 次})$

$a^{n+1} = -(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n) a$

$= -(p_1 a^n + \cdots + p_{n-1} a^2 + p_n a)$

$= -1 \{p_1(-(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n)) + \cdots + p_{n-1} a^2 + p_n a\} \quad (n-1 \text{ 次})$

$b^{m+1} = -\{q_1(-(q_1 b^{m-1} + \cdots + q_{m-1} b + q_m) + \cdots + q_{m-1} b^2 + q_m b\} \quad (m-1 \text{ 次})$

体 $Q(a, b)$ は $a^k, b^h, a^k b^h$ の一次結合であるから，高々 $n, m, n + m + nm$ 次の線形空間だあるから

$$a + b, \ a - b, \ ab, \ a/b \in Q(a, b)$$

（注）有理数体は最小の数体である.

2) 代数拡大と作図可能性

作図は，与えられた実数から四則演算と開平の操作を有限回続けて，新しい実数を求めることであった.

定　義　二つの体 F，K について $F \subset K$ となるとき，K を F の拡大体，F を K の部分体という.

定　義　K の F 上線形空間としての次数を K の F 上拡大次数といい，$[K : F]$ と記す.

定　理　実数 $a_1, a_2, a_3, \cdots, a_n$ で定まる図形から，定規とコンパスで作図できる新しい図形を定める実数を u とするとき，

$$[K : F] = 2^p \quad (p : \text{正の整数})$$

証　明　$K(u) \subset K(u_1, u_2, u_3, \cdots, u_m)$

$u_1^2 \in K, \quad u_i^2 \in K(u_1, u_2, u_3, \cdots, u_{i-1})$

$\therefore [K(u_1, u_2, u_3, \cdots, u_i) : K(u_1, u_2, u_3, \cdots, u_{ii-1})] = 1 \ or \ 2$

$[K(u) : K] = [K(u) : K(u_1)] \times [K(u_1) : K(u_1, u_2)] \times \cdots \times [K(u_1, u_2 \cdots) : K]$

$\therefore [K : F] = 2^p \quad (p : \text{正の整数})$

この定理を用いて，ギリシャ時代の難問(1)，(2)は次のように説明される.

(1)　角を三等分することは，$a = \cos 3\theta$ を与えて $\cos \theta$ を求めることである.

$cos\ 3\theta = 4cos^3\ \theta - 3cos\theta$　だから $2\ cos\ \theta = u$　とおくと

$u^3 - 3u - 2a = 0$

$\theta = 20^\circ$　とおくと　$a = \dfrac{1}{2}$

$\therefore\ u^3 - 3u - 1 = 0$,　Q：既約

$\therefore\ [Q(u) : Q] = 3$　よって，u は作図不可能である．

(2)　立方体の一辺を a　を与えて，$u^3 - 2 = 0$ を求めることである．

$a = 1$　とおくと　$u^3 - 2 = 0$,　Q：既約

$\therefore\ [Q(u) : Q] = 3$　よって，u は作図不可能である．

（注）(1) は，1837 年に Wantzel という人がこの方法で証明した．

(3) は，1882 年に Lindeman が π　は代数的数でないことを証明して解決された．

3. 累乗根拡大と巡回群

$x_1, x_2, x_3, \cdots, x_n$ を根にもつ　n　次方程式を次のようにおく，

$$x^n + s_1 x^{n-1} + s_2 x^{n-2} + \cdots + s_n = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(*)$$

ただし，係数 $s_1, s_2, s_3, \cdots, s_n$ は，根 $x_1, x_2, x_3, \cdots, x_n$ の基本対称式である．

即ち，

$$x_1 + x_2 + x_3 + \cdots x_n = -s_1$$

$$x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_{n-1}x_n = s_2$$

$$\cdots$$

$$x_1x_2x_3\cdots x_n = (-1)^n s_n$$

方程式（＊）の根の公式を求めることは，根 $x_1, x_2, x_3, \cdots, x_n$ を四則演算と累乗根を用いて方程式の係数 $s_1, s_2, s_3, \cdots, s_n$ から求めることである．そのために，まず有理数体を次のように拡大していく必要がある．

(1) 累乗根拡大

F を有理数体とする．

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

$$Fi_{+1} = Fi(\sqrt[p_i]{a_i}),\quad a_i \in F_i,\quad p_i：素数,\quad \sqrt[p_i]{a_i} \notin F_i$$

(2) 方程式の根の公式は，根　$x_1, x_2, x_3, \cdots, x_n$ の基本対称式で表されるから，根の循環置換で不変である．

定　理　F を体，$p(x)$ を既約な F 係数の多項式とする．　$p(x)$ を法とする類の全体を K とする．

$$K = F[x] / p(x)$$

$p(x)$ の根は K の元であり，x　の類を a　とすると，は a　の　$p(x)$ 根である．

証　明　　$a = x \ (mod\ p(x))$ とおくと

$$p(a) = p(x) \ (mod\ p(x)) = 0$$

$\therefore\ a$ は $p(x)$ の根

$\therefore\ p(x) = (x-a)p_1(x)$　ただし，$p_1(x)$ は既約多項式

（注）実際　$p(x) = (x-a)p_1(x)$ のとき，x を $p(x)$ で割ると次の計算のように剰余が $p(x)$ の根 a であることが容易にわかる．

$$\begin{array}{r|l} & 1 \\ \hline x-a & x \\ & x-a \\ \hline & a \end{array}$$

$F_1 = F[x] \ / \ p_1(x)$

$a_1 = x \ (mod\ p_1(x))$　とおくと

$p(x) = (x-a)(x-a_1)p_2(x)$　ただし，$p_2(x)$ は既約多項式

以下同様に続けていくと，次のことがわかる．

定　理　F: 任意の体 F の拡大体を K とする．$p(x)$ を F 上既約多項式とする．
$p(x)$ は，次のように K 上の一次多項式の積に分解する．

$$p(x) = (x-a)(x-a_1)(x-a_2)\cdots(x-a_n)$$

$$a,\ a_1,\ a_2,\ \cdots,\ a_n \in K$$

定　義　F 係数の多項式 $p(x)$ が，F 上の拡大体 K で一次多項式の積に分解されるとき，K を $p(x)$ の分解体という．

4. 正規部分群の役割

1) 剰余類

定　理　H：群 G の部分群とするとき, G は次のように分割できる．

$$G = a_1H \cup a_2H \cup a_3H \cup \cdots \cup a_nH$$

証　明　　$aH \cap bH \neq \varnothing$ のとき，

$x \in aH \cap bH$ とおくと，$x = ah_1 = bh_2$ ($h_1,\ h_2 \in H$)

$a = b\ h_2\ h_1^{-1}$ ($h_1,\ h_2 \in H$)

$\therefore\ aH = bH$

$\therefore\ aH \cap bH = \varnothing\ or\ aH = bH$

これを　$G = a_1H + a_2H + \cdots + a_nH$ と記す．

2) 正規部分群（不変部分群）

定　義　H：群 G の部分群とする.

G の任意の元 g に対して, $gHg^{-1} = H$ が成り立つとき, H を G の正規部分群という.

（注）G：可換群のとき. G の全ての部分群は正規部分群である.

3) 剰余類群（商群）

定　理　H ： 群 G の正規部分群とするとき, $\{a_1H,\ a_2H,\ a_3H,\ \cdots,\ a_nH\}$ は群を成す.

証　明　$(gH)(g'H) = gg'H$

$(eH)(gH) = gH$

$\therefore\ eH = H$ (単位元)

$(gH)(g^{-1}H) = H$

$\therefore\ (gH)^{-1} = g^{-1}H$ (逆元)

定　義　この群を剰余類群（商群）といい, G / H と記す.

4) 固定群（不動群）

方程式 $f(x) = 0$ の係数も根の公式も, 根 $x_1,\ x_2,\ x_3,\ \cdots,\ x_n$ の置換で不変である.

そこで, 次に述べる不動群, 不動体という概念が必要になる.

定　義　F：基礎体とする. F を含む K の部分体 E を, F と K の中間体という.

$F \subset E \subset K$

E の元を不動にする同型写像　σ　を E 上同型写像という.

$\sigma(x) = x \quad (x \in E)$

定　義　E 上同型写像の全体は群を成し, E の固定群 H という.

$H = G(E) = \{\sigma \in G \mid \sigma(x) = x,\ x \in E\}$

（注）　F, K の固定群をそれぞれ $G = G(F),\ I = G(K)$ とすると

$G \supset H \supset I,\ (\ I = \{e\}\ )$

	対　応	
K(I) = K	……	I = G (K)
∪	対　応	∩
K(H) = E	……	G(E) = H
∪	対　応	∩
K(G) = F	……	G = G(F)

定　理　有理数体 Q は同型写像 σ　で不動である.

証　明　n：自然数のとき,

$$\sigma(n) = \sigma(1 + 1 + 1 + \cdots + 1)$$

$$= \sigma(1) + \sigma(1) + \sigma(1) + \cdots + \sigma(1)$$

$$= 1 + 1 + 1 + \cdots + 1$$

$$= n$$

$$r = \pm \frac{n}{m} \quad (m,\ n\ :\ \text{自然数})$$

$$\sigma(r) = \sigma\left(\pm \frac{n}{m}\right) = \pm \frac{\sigma(n)}{\sigma(m)} = \pm \frac{n}{m} = r$$

定　理　K　上の代数的数 α　は, 同型写像により K 上の共役数に写される.

証　明　　$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$,　　$a_1, a_2, a_3, \cdots, a_n \in K$ とする.

$$f(\alpha) = \alpha^n + a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \cdots + a_n = 0$$

$$\sigma(f(\alpha)) = \sigma(\alpha^n + a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \cdots + a_n)$$

$$= \sigma(\alpha)^n + a_1 \sigma(\alpha)^{n-1} + \cdots + a_n$$

$$= f(\sigma(\alpha)) = 0$$

$\therefore$ σ(α)：$f(x)$ の根

5. ガロア拡大

定　義　　基礎体 F の分離拡大体を K とするとき, K の F 上の全ての共役体が一致するとき, K を F のガロア拡大体 G といい, G = Gal(K/F) と記す.

（注）　K = F(α) で　α のF上の共役根を $\alpha = \alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$ とすると

$$K = F(\alpha) = F(\alpha_2) = F(\alpha_3) = \cdots = F(\alpha_n)$$

K は αの全ての共役根を含んでいる.

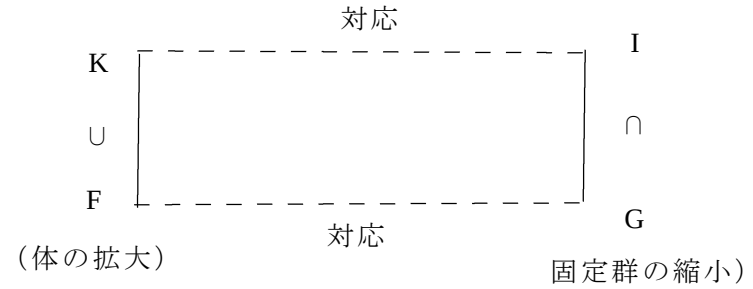
1)　体 F の拡大を次のようにとる.

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_k = K$$

2)　体 G の部分体 F_i　の固定群を $G(F_i) = H_i$ とすると,

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_k = I = \{e\}$$

$$H_i \ |> \ H_{i+1}$$



3) α の F 上最小多項式を $f(x)$ とすると，K は $f(x)$ の分解体である．

K は分離拡大体だから，次の条件を満たすことが G が可解群であるための必要十分条件である．

(1) $H_i \mid> H_{i+1}$

(2) H_i / H_{i+1} の位数が素数

引用文献

1. Renè Descartes, The Geometry of Rene Descartes,
translated by David Smith and Marcia L. Lathan, Dover, 1954
2. Ian Stewart, Galois Theory, Chapman and Hall, 1972
3. 安部　斉 著　　代数ことはじめ　森北出版 1993
4. 東郷　重明 著　代数入門　　サイエンス社 2001
5. 石田　信 著　　代数学入門　実教出版 1999
6. 草場　公邦 著　ガロワと方程式　朝倉書店 2004
7. 渡辺　敬一, 草場　公邦 著　代数の世界　朝倉書店 2004
8. 松村　英之　著　代数学　朝倉書店 1990