# ガロア理論（Galois Theory）

## 目 次



## 1 まえがき

線形代数（ベクトル空間，次元など）と群論の初歩的な知識は仮定する．

## 2 環，整域，体，イデアル，多項式

加法と乗法の 2 つの演算が定められていて以下の公理を満足する集合 $R$ を **環** という．

- 加法に関してアーベル群[1]である．
- 乗法に関して半群[2]である．
- 加法と乗法に関して分配法則 $x(y+z) = xy + xz$，$(x+y)z = xz + yz$ を満たしている．

**命題 1.** 環 $R$ においては $x0 = 0x = 0$, $(-x)y = x(-y) = -(xy)$, $(-x)(-y) = xy$ が成り立つ．

*Proof.* $x0 + x0 = x(0+0) = x0$ より $x0 + x0 = x0$ で，この両辺に $-(x0)$ を足して $x0 = 0$ をえる．$0x = 0$ も同様に示せる．
$xy + (-x)y = (x + (-x))y = 0y = 0$ より $(-x)y = -(xy)$．同様にして $x(-y) = -(xy)$ も示せる．
$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy.$ □

[1] 交換法則 $x + y = y + x$ を満たす群.
[2] 結合法則 $(xy)z = x(yz)$ を満たしていること．

とくに，乗法に関して交換法則 $xy = yx$ を満たしている環は **可換環** とよばれる．0 でない乗法単位元 1 をもつ環は **単位的** とよばれる．

単位的可換環 $R$ は $R$ の 0 でない 2 つの元の積はやはり 0 にならないとき **整域** とよばれる．

次の命題は容易に示せるが有用である．

**命題 2.** 単位的可換環 $R$ が整域であるためには，次の消約律が成り立つことが必要十分である：

$$a \neq 0,\ ax = ay \Rightarrow x = y.$$

0 でない元の全体が乗法に関してアーベル群となっている環 $K$ を **体** という[3]．

**命題 3.** 体は整域である．

*Proof.* 体は単位的可換環である．$x \neq 0 \neq y$ とすると $(xy)(y^{-1}x^{-1}) = 1 \neq 0 = 0(y^{-1}x^{-1})$ であることから $xy \neq 0$ となる．
別証明．体は単位的可換環である．$a \neq 0$，$ax = ay$ とすると，両辺に左から $a^{-1}$ を乗じて $x = y$．よって消約律が成り立つので整域である． □

**命題 4.** 有限な整域は体である．

*Proof.* $R$ を $\sharp R < \infty$ である整域，$a$ を $R$ の 0 でない元とする．写像 $R \ni x \mapsto ax \in R$ は消約律により単射であり，$\sharp R < \infty$ より全射となる．よってある $x \in R$ が存在して $ax = 1$. 単位的可換環 $R$ の非ゼロ元が乗法的逆元をもつので $R$ は体である． □

**例．** 整数の集合 $\mathbb{Z}$ は通常の加法と乗法により整域で，有理数の集合 $\mathbb{Q}$，実数の集合 $\mathbb{R}$，複素数の集合 $\mathbb{C}$ は体である．

環 $R$ の部分集合 $I$ は次を満たしているとき $R$ の **イデアル** という．

- 加法に関して部分群となっている．
- 吸収法則 $ra \in I$, $ar \in I$ $(a \in I, r \in R)$ を満たしている．

環 $R$ のいくつかのイデアルの共通部分も再びイデアルとなる．よって，$X$ を環 $R$ の部分集合とするとき，$X$ を含むすべてのイデアルの共通部分はイデアルで，$X$ で **生成される** $R$ の **イデアル** といい $(X)$ で表す[4]．$R$ の有限部分集合 $\{x_1, \ldots, x_k\}$ で生成されるイデアルは $(x_1, \ldots, x_k)$ とかく．$R$ のイデアル $I$ がその有限部分集合で生成されるとき，**有限生成のイデアル** という．1 元集合 $\{x\}$ で生成されるイデアル $I = (x)$ を $x$ で生成される **単項イデアル** という．すべてのイデアルが単項イデアルである環を **単項イデアル環**，単項イデアル環である整域を **単項イデアル整域**（PID[5]）という．

**命題 5.** $R$ を単位的な可換環，$X$ を $R$ の部分集合とすると，$(X) = RX = \left\{ \sum_{i=1}^{k} r_i x_i \,|\, r_i \in R, x_i \in X \right\}$.

*Proof.* Exercise. □

**定理 1.** 整数の整域 $\mathbb{Z}$ は単項イデアル整域で，どのイデアルも $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$（$n$ は非負の整数）というカタチをしている．また，この $n$ は一意的である．

[3] 平たくいえば，0 による除法を除いて四則演算が自由にできる集合ということである．ドイツ語で体を Körper ということから，体を表すのにアルファベットの大文字 K がよく使われる．
[4] $X$ を含む最小のイデアルになる．
[5] Principal Ideal Domain の略．

*Proof.* ゼロイデアル $\{0\}$ は $0\mathbb{Z}$ で単項なので，$I$ を $\mathbb{Z}$ のゼロイデアルでないイデアルとする．$I$ は 0 でない整数 $n$ を含み $-n$ も含むので必ず正の整数を含む．$n$ を $I$ に属する最小の正の整数とする．$m \in I$ として $m$ を $n$ で割り算することにより $m = qn + r$ $(q, r \in \mathbb{Z}, 0 \leq r < n)$ と書けることになる．すると $r = m - qn \in I$ で，$n$ は $I$ に属する最小の正の整数と仮定したから $r = 0$．よって $m = qn$ と書けることになり $I \subset n\mathbb{Z}$．逆の包含はあきらかなので $I = n\mathbb{Z}$ となる．一意性はあきらかである． □

環 $R$ において $\{0\}$ と $R$ はイデアルであるがこれらは **自明なイデアル** とよばれる．

**命題 6.** 単位的可換環 $R$ が体であるための必要十分条件は，$R$ が自明でないイデアルをもたないことである．

*Proof.* $R$ を体，$I$ を $R$ の $\{0\}$ でないイデアルとする．$I$ は 0 でない元 $a$ を含むので $1 = a^{-1}a \in I$ であり，$I = R$ であることになる．

逆に単位的可換環 $R$ が自明でないイデアルをもたないとする．もしも $a \neq 0$ であれば $(a) = R$ であるから $ab = 1$ となる $b \in R$ が存在することになる． □

$I$ を環 $R$ のイデアルとすると $I$ は加法群としての $R$ の部分群なので剰余群 $R/I$ を構成できる．すなわち，剰余類 $x + I$ を $\overline{x}$ と書くとき $R/I = \{\overline{x} \mid x \in R\}$ は演算

$$\overline{x} + \overline{y} = \overline{x + y}$$

によってやはり加法群となる．さらに次の命題により乗法を

$$\overline{x}\ \overline{y} = \overline{xy}$$

として定義することができる．

**命題 7.** $\overline{x}\ \overline{y} = \overline{xy}$ は *well defined* である．

*Proof.* $\overline{x} = \overline{x'}$，$\overline{y} = \overline{y'}$ とすると $xy - x'y' = x(y - y') + (x - x')y' \in I$． □

この自然な加法と乗法により $R/I$ は再び環となり $R$ の $I$ による **剰余環** とよばれる．

**命題 8.** $p$ が素数のとき剰余環 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ は体である．

*Proof.* $\mathbb{Z}_p \ni \overline{a} \neq \overline{0}$ とすると $p$ と $a$ は互いに素であるから $c, d \in \mathbb{Z}$ が存在して $cp + da = 1$．すると $\overline{da} = \overline{1}$ となり $\overline{d}$ は $\overline{a}$ の乗法的逆元である． □

環 $R$ から環 $S$ への写像 $\phi : R \longrightarrow S$ が加法と乗法を保つ，すなわち

$$\phi(x + y) = \phi(x) + \phi(y)\,,\quad \phi(xy) = \phi(x)\phi(y)$$

であるとき $R$ から $S$ への **準同形**（または **環準同形**）という．但し，$R$ も $S$ も単位的であるときは $\phi(1) = 1$ も条件に加える[6]．

環 $R$ の部分集合 $S$ が，加法に関して部分群で乗法に関して部分半群であるとき，$R$ の **部分環** という．但し，$R$ が単位的であるときは $1_R \in S$ も条件に加える．

環準同形 $\phi : R \longrightarrow S$ に対して加法群準同形としての核

$$\mathrm{Ker}\,\phi = \{x \in R \mid \phi(x) = 0\}$$

は $R$ のイデアルで[7]，像 $\mathrm{Im}\,\phi = \phi(R)$ は $S$ の部分環となっている．

全単射である環準同形を **同形**（または **環同形**）もしくは **同形写像**（または **環同形写像**）という．環同形の逆写像も環同形となる．環 $R$ から環 $S$ への同形があるとき $R$ と $S$ は **同形** といい $R \cong S$ と表す．

[6]左側の 1 は $R$ の単位元 $1_R$，右側の 1 は $S$ の単位元 $1_S$ である．

[7]逆に $R$ のイデアル $I$ は自然な全射準同形 $\pi : R \longrightarrow R/I$，$\pi(x) = x + I$，の核となっている．

**定理 2 (環準同形定理).** $\phi : R \longrightarrow S$ を環準同形とすると剰余環 $R/\mathrm{Ker}\,\phi$ と像 $\mathrm{Im}\,\phi$ は自然に同形である.

*Proof.* 写像 $x + \mathrm{Ker}\,\phi \longmapsto \phi(x)$ が同形となることが群の準同形定理と同様に示すことができる. □

$R$ を環, $r \in R$ とする. 正の整数 $n$ について $n.r$ を帰納的に $1.r = r$, $n.r = (n-1).r + r$ $(n \geq 2)$ と定める. また, $0.r = 0$, $(-n).r = -(n.r)$ ($n$ は正の整数) と定める. このとき $m, n \in \mathbb{Z}$, $r, s \in R$ に対して,

$$(m+n).r = m.r + n.r\,, \quad n.(r+s) = n.r + n.s$$

$$(mn).r = m.(n.r)\,, \quad (m.r)(n.s) = (mn).(rs)$$

が成り立つ. とくに $R$ が単位的な環のとき, 写像 $\mu : \mathbb{Z} \longrightarrow R$, $n \longmapsto n.1$, は環準同形で[8]定理 1 よりある非負の整数 $n$ で $\mathrm{Ker}\,\mu = n\mathbb{Z}$ となるのが一意的に存在する. この非負の整数 $n$ を $R$ の **標数** とよび $\mathrm{char}R$ で表す[9].

**命題 9.** 整域 $R$ の標数は 0 もしくは素数である.

*Proof.* $\mathrm{char}R \neq 0$ とする. $n = \mathrm{char}R$ とすると $n$ は 1 ではありえないから $n \geq 2$ である. $n = n'n''$ ($n'$, $n''$ は 2 以上の整数) と表せるとすると $n.1 = (n'.1)(n''.1) = 0$ となり, $R$ が整域であることから $n'.1 = 0$ または $n''.1 = 0$. これは $n$ を標数としたことに反する. よって $n$ は素数ということになる. □

$R$ を可換環とする. $R$ に係数をもつ（もしくは $R$ 上の） **不定元** $x$ の（1 変数）**多項式** $f(x)$ とは $n$ を非負の整数として

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \quad (a_i \in R)$$

というカタチのモノである. 2 つの多項式の相等は通常のように定められる. $a_i \neq 0$ となる最大の $i$ を多項式 $f(x)$ の **次数** といい $\deg f(x)$ で表す. 便宜上, 多項式 0 の次数は $-\infty$ と定める[10].

$a_k = 0$ であるとき **項** $a_k x^k$ は省略してもよいことにする. 0 次の多項式および 0 を **定数**（多項式）という. 定数は $R$ の元と同一視できる.

2 つの多項式に対して加法と乗法を

$$\sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} b_j x^j = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n} c_k x^k$$

但し, $\max(m,n)$ は $m$ と $n$ の小さくない方で $c_k = \sum_{i+j=k} a_i b_j$, と定めると $R$ に係数をもつ不定元 $x$ の多項式の全体 $R[x]$ も可換環となり, $R$ 上の（$x$ を不定元とする 1 変数）**多項式環** という.

[8] $\mathbb{Z}$ から $R$ への環準同形はこの $\mu$ に限ることも示せる.

[9] 要するに $n.1 = 0$ となる最小の正の整数 $n$ があればその $n$ が標数で, そのような $n$ が存在しなければ 0 が標数ということになる. char は characteristic の略.

[10] $-\infty < 0$, $-\infty + n = -\infty$ などとする.

**命題 10.** $f, g \in R[x]$ に対して次の公式が成り立つ.

(i) $\deg(f+g) \leq \max(\deg f, \deg g)$.

(ii) $\deg(fg) \leq \deg f + \deg g$. $R$ が 整域のときは等号が成り立つ.

**命題 11.** $R$ が整域ならば $R[x]$ も整域である.

*Proof.* 命題 10 の 2 番目から従う. □

**命題 12 (割り算アルゴリズム).** $K$ を体, $g \in K[x]$, $g \neq 0$ とする. このとき任意の $f \in K[x]$ に対してある $q, r \in K[x]$ で $f = qg + r$（$\deg r < \deg g$）となるのが一意的に存在する[11].

*Proof.* $\deg f = m$, $\deg g = n$ として, まず存在を $m$ についての帰納法で示す. $m < n$ のときは $q = 0$, $r = f$ とすればよい. $m \geq n$ のとき. $f$ の最高次の係数を $a_m$, $g$ の最高次の係数を $b_n$ とする. $f_1 = f - \dfrac{a_m}{b_n} x^{m-n} g$ とすると $\deg f_1 < m$ で帰納法の仮定から $f_1 = q_1 g + r_1$, $\deg r_1 < n$ となる $q_1, r_1 \in K[x]$ が存在する. よって, $f = \left( q_1 + \dfrac{a_m}{b_n} x^{m-n} \right) g + r_1$ となる.

次に一意性を示す. $f = qg + r = q'g + r'$, $\deg r < n$, $\deg r' < n$ とすると, $(q - q')g = r' - r$ で $q \neq q'$ とすると $\deg((q - q')\, g) \geq n$, $\deg(r' - r) < n$ で矛盾. よって $q = q'$. ゆえに $r' - r = 0$. よって $r = r'$. □

この命題で $r = 0$ となるとき $f$ は $g$ で **割り切れる** とよび, $g$ を $f$ の **因子** という.
定理 1 と同様にして次が示される.

**定理 3.** 体 $K$ 上の多項式環 $K[x]$ は単項イデアル整域である.

**例題 .** $\mathbb{Z}[x]$ は単項イデアル整域ではないことを示せ.

Sol. イデアル $(2, x)$ が単項イデアルでないことを示す. $f \in \mathbb{Z}[x]$ が存在して $(2, x) = (f)$ とすると $f \mid 2$ かつ $f \mid x$. よって $f$ は 1 か $-1$ である. $(1) = (-1)$ なので $(1) \neq (2, x)$ を云えばよい. $1 = 2g + xh$ とすると $1 = 2g(0)$ となり不合理である.

体 $K$ を係数とする多項式 $f_1, \ldots, f_k$ は, それらすべてを割り切る $K$ 上の定数でない多項式が存在しないとき, **互いに素** であるという.

**命題 13.** $K$ を体とするとき, $f_1, \ldots, f_k \in K[x]$ が互いに素ならば, ある $g_1, \ldots, g_k \in K[x]$ で

$$f_1(x)g_1(x) + \cdots + f_k(x)g_k(x) = 1$$

となるのが存在する.

*Proof.* $I = (f_1, \ldots, f_k)$ とすると, 定理 3 よりある $d \in K[x]$ が存在して $I = (d)$. すると $d$ は互いに素な $f_1, \ldots, f_k$ をすべて割り切るので定数で $I = K[x]$ であることになる. よって命題 5 により所望の多項式 $g_1, \ldots, g_k$ が存在することになる. □

$K$ を体とするとき, 定数でない $f \in K[x]$ が $f$ より次数の低い定数でない多項式で割り切れないとき, $f$ を $K$ 上で **既約** という[12]. $K$ 上で既約でないとき $K$ 上で **可約** という.

**命題 14.** $K$ を体, $f, g, h \in K[x]$ とする. $f$ が $K$ 上で既約で積 $gh$ を割り切るならば $f$ は $g$ もしくは $h$ を割り切る.

[11] $q$ は **商**, $r$ は **剰余** とよばれる.
[12] どちらも低次な 2 つの多項式の積とならないこと, といってもよい.

*Proof.* $f$ が $g$ を割り切らないと仮定する．$f$ と $g$ を割り切る $K[x]$ の定数でない元があったとすると，それは $f$ の定数倍で $g$ を割り切ることになり，$f$ が $g$ を割り切ることになってしまう．これは仮定に反するので $f$ と $g$ は互いに素ということになる．よって，命題 13 より，ある $u, v \in K[x]$ が存在して $ug + vf = 1$．すると $ugh + vfh = h$ となり $f$ は $h$ を割り切ることになる． □

**命題 15.** $f$ を体 $K$ 上の既約多項式とすると，剰余環 $K[x]/(f)$ は体である．

*Proof.* $I = (f)$ とおく．$K[x]/I$ は可換で乗法単位元 $1+I$ をもつ．$g+I \neq I$ とすると $g \notin I$ であることから $g$ は $f$ で割り切れないので，$f$ と $g$ を割り切るのは定数に限ることになり $f$ と $g$ は互いに素ということになる．よって，命題 13 より，ある $h, k \in K[x]$ が存在して $fh + gk = 1$．すると，$fh \in I$ であるから，$(k+I)(g+I) = 1+I$ となり，$k+I$ は $g+I$ の乗法逆元となる．よって $K[x]/I$ の非ゼロ元は逆元をもつので $K[x]/I$ は体ということになる． □

整数係数の多項式 $f = \sum_{i=0}^{n} a_i x^i$ の係数が互いに素であるとき，$f$ を **原始多項式** という．整数係数の多項式 $f = \sum_{i=0}^{n} a_i x^i$ に対して，$a_0, \ldots, a_n$ の最大公約数を $b$ とすると，$a_i = bc_i$ $(c_i \in \mathbb{Z})$ として $f = b\sum_{i=0}^{n} c_i x^i$ と表したときの $\sum_{i=0}^{n} c_i x^i$ は原始多項式で，これを $f$ に **属する原始多項式** という．

環準同形 $\sigma : R_1 \longrightarrow R_2$ は環準同形 $\sigma_* : R_1[x] \longrightarrow R_2[x]$, $\sigma_*(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \sigma(a_i) x^i$, を導く．$\sigma$ が同形であれば $\sigma_*$ も同形である．

$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ を剰余類を対応させる自然な全射準同形とするとき，$f \in \mathbb{Z}[x]$ に対して $\pi_*(f)$ を $(f)_n$ と書くことにする．

**命題 16 (ガウスの補題).** 原始多項式の積は原始多項式である．

*Proof.* $f$, $g$ を原始多項式とする．もしも $fg$ が原始多項式でないとするとある素数 $p$ があって $(fg)_p = 0$．一方，$(fg)_p = (f)_p (g)_p \neq 0$．これは矛盾． □

**命題 17.** $\mathbb{Z}$ 上で既約な多項式 $f \in \mathbb{Z}[x]$ は $\mathbb{Q}$ 上でも既約である．

*Proof.* $f$ は原始的と仮定してよい．$f = gh$ $(g, h \in \mathbb{Q}[x],\ \deg g, \deg h < \deg f)$ と分解できるとする．$g$ に正の有理数 $a$ を乗じて $ag$ は整数係数で原始的とでき，$h$ についても正の有理数 $b$ を乗じて $bh$ は整数係数で原始的とできる．$abf = (ag)(bh) = \varphi$ は原始的である．$ab = n/m$ $(m,\ n$ は正の整数，既約分数$)$ として，$(n/m)f = \varphi$ より $nf = m\varphi$. $f = \sum_{i=0}^{k} a_i x^i$, $g = \sum_{i=0}^{k} b_i x^i$ とおくと，$na_i = mb_i$ $(0 \leq i \leq k)$ かつ $(na_0, \ldots, na_k) = (n) = (mb_0, \ldots, mb_k) = (m)$．よって $n/m = ab = 1$．よって $abf = f = (ag)(bh)$ となり $f$ は $\mathbb{Z}$ 上で可約ということになる． □

**命題 18 (アイゼンシュタインの既約性判定基準).** $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, $\deg f(x) = n \geq 1$, $p$ は素数とする．$p$ は $a_n$ の約数でなく $a_0, a_1, \ldots, a_{n-1}$ の約数で，$p^2$ は $a_0$ の約数でないとする．このとき $f$ は有理数の体 $\mathbb{Q}$ 上で既約である．

*Proof.* $f$ に属する原始多項式 $g = b_0 + b_1 x + \cdots + b_n x^n$ が $\mathbb{Z}$ 上で既約なことを示せばよい．$p \mid b_i (i = 0, 1, \ldots, n-1)$, $p \nmid b_n$, $p^2 \nmid b_0$ であることは容易にわかる．$g = g_1 g_2 (g_i \in \mathbb{Z}[x],$ $\deg g_i < \deg g)$ と分解されたとする．$(g)_p = (b_n)_p x^n = (g_1)_p (g_2)_p$ である．$g_1$ は $s$ 次で $g_1 = \sum_{i=0}^{s} c_i x_i$, $g_2$ は $t$ 次で $g_2 = \sum_{i=0}^{t} d_i x_i$ と置くと，$(g_1)_p = (c_s)_p x^s$, $(g_2)_p = (d_t)_p x^t$, $s + t = n$ なので $i \neq s$ のとき $c_i \equiv 0 \pmod{p}$, $j \neq t$ のとき $d_j \equiv 0 \pmod{p}$．ところが $b_0 = c_0 d_0 \equiv 0 \pmod{p}$ なので $c_0 \equiv 0 \pmod{p}$ と仮定してよい．また $p^2 \nmid b_0$ より $d_0 \not\equiv 0 \pmod{p}$．よって $0 = t$, $s = n$ で $\deg g_1 = n$ となり矛盾． □

**例題．** $p$ 次円分多項式 $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$（$p$：素数）は $\mathbb{Q}$ 上既約であることを示せ.

Sol. $(1-x)\Phi_p = 1-x^p$ である．$x = 1+y$ と置くと $1-x^p = 1-(1+y)^p = -y\sum_{i=1}^{p}\binom{p}{i}y^{i-1} = (1-x)\sum_{i=1}^{p}\binom{p}{i}y^{i-1}$．$\mathbb{Q}[x]$ は整域ゆえ $\Phi_p = \sum_{i=1}^{p}\binom{p}{i}y^{i-1}$．アイゼンシュタインの判定基準から $\sum_{i=1}^{p}\binom{p}{i}y^{i-1}$ は既約なので，対偶を考えると $\Phi_p$ も既約である.

## 3　体の拡大，作図問題

体 $K$ と体 $L$ について $K$ が $L$ の部分環であるとき $K$ を $L$ の **部分体**，$L$ を $K$ の **拡大体** という．またこの状況を **拡大** $L/K$ とよぶ.

拡大 $L/K$ が与えられると $L$ は自然に $K$ 上のベクトル空間となる．この次元 $\dim_K L$ を **拡大次数** とよび $[L:K]$ で表す．$[L:K]$ が有限なとき拡大 $L/K$ を **有限次拡大** という.

$M/L$，$L/K$ が体の拡大のとき $L$ を $M/K$ の **中間体** とよぶ.

**命題 19 (タワー公式).** $L$ が $M/K$ の中間体であるとき，拡大 $M/K$ が有限次である必要十分条件は $M/L$ も $L/K$ も有限次であることで，このとき $[M:K] = [M:L][L:K]$ が成立する.

*Proof.* $M/K$ を有限次拡大とする．$L$ は $K$ 上有限次元のベクトル空間 $M$ の部分空間であるから $K$ 上有限次元のベクトル空間であり $L/K$ は有限．また，$[M:K]$ が有限であることから $K$ 上のベクトル空間としての $M$ の有限生成系があるが，これは $L$ 上のベクトル空間としての $M$ の生成系でもあり $[M:L]$ は有限でなければならない.

逆に $M/L$ も $L/K$ も有限次拡大とする．$M$ の $L$ 上の基底を $x_1, \ldots, x_m$，$L$ の $K$ 上の基底を $y_1, \ldots, y_n$ とする．このとき積 $x_i y_j$ $(1 \le i \le m, 1 \le j \le n)$ の全体は $M$ の $K$ 上の基底となるので，$[M:K]$ は有限で $[M:K] = [M:L][L:K]$ となる．□

ユークリッド平面の点 $(0,0)$，$(1,0)$ から次によって帰納的にえられるユークリッド平面の点を（初等的に）**作図可能な点** とよぶ.

- 作図可能な 2 点をむすぶ直線 2 本の交点.
- 作図可能な 2 点をむすぶ直線と作図可能な点を中心とし別の作図可能な点を通る円との交点.
- 作図可能な点を中心とし別の作図可能な点を通る 2 円の交点.

**定理 4.** ユークリッド平面の作図可能な点 $(x,y)$ に対して，$[\mathbb{Q}(x,y):\mathbb{Q}]$ は 2 のべきである.

*Proof.* $P_0 = (0,0)$, $P_1 = (1,0)$ とし，$P_0, P_1, \ldots, P_n$ が定義によって順次定まる作図可能な点で $P = P_n$ とする．$P_i = (x_i, y_i)$ として，帰納的に $K_0 = K_1 = \mathbb{Q}$，$K_j = K_{j-1}(x_j, y_j)$ $(2 \le j \le n)$ と定める．各 $j$ について，$x_j$ も $y_j$ も $K_{j-1}$ に係数をもつ 1 次か 2 次の多項式の根[13]であるから，$[K_{j-1}(x_j):K_{j-1}] = 1$ または 2 かつ $[K_{j-1}(x_j,y_j):K_{j-1}(x_j)] = 1$ または 2 である．したがって，タワー公式により $[K_n:\mathbb{Q}]$ は 2 のべきで，$[K_n:\mathbb{Q}] = [K_n:\mathbb{Q}(x,y)][\mathbb{Q}(x,y):\mathbb{Q}]$ なので $[\mathbb{Q}(x,y):\mathbb{Q}]$ も 2 のべきでなければならないことになる．□

**系 1.** 定規とコンパスによる通常の方法では $\dfrac{\pi}{3}$ $(= 60^\circ)$ の 3 等分の作図は不可能である.

[13] 多項式 $f$ に対して $f(\alpha) = 0$ である $\alpha$ を $f$ の **根** という.

*Proof.* $a = \cos\dfrac{\pi}{9}$, $b = \sin\dfrac{\pi}{9}$ とする．点 $(\cos\dfrac{\pi}{3}, \sin\dfrac{\pi}{3})$ は作図可能なので定規とコンパスによる通常の方法で $\dfrac{\pi}{3}$ の 3 等分の作図が可能とすると点 $(a,b)$ が作図可能ということになる．3 倍角の公式 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ で $\theta = \dfrac{\pi}{9}$ として $4a^3 - 3a = \dfrac{1}{2}$．よって $8a^3 - 6a - 1 = 0$．$f(x) = x^3 + 3x^2 - 3$ とすると $8a^3 - 6a - 1 = f(2a-1)$ である．アイゼンシュタインの判定基準から $f$ は $\mathbb{Q}$ 上で既約なので $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(2a-1) : \mathbb{Q}] = 3$. よって定理 4 により点 $(\cos\dfrac{\pi}{9}, \sin\dfrac{\pi}{9})$ は作図不能である．したがって定規とコンパスによる通常の方法では $\dfrac{\pi}{3}$ の 3 等分の作図は不可能である． □

$L/K$ を体の拡大，$\alpha$ を $L$ の元とする．ある 0 でない $f \in K[x]$ で $f(\alpha) = 0$ となるのが存在するとき $\alpha$ は $K$ 上 **代数的**，そうでないとき $K$ 上 **超越的** という．$L$ のどの元も代数的なとき拡大 $L/K$ を **代数的拡大** という．

**命題 20.** 有限次拡大は代数的拡大である．

*Proof.* $L/K$ を有限次拡大，$n = [L : K]$，$\alpha \in L$ とする．$n+1$ 個の元 $1, \alpha, \alpha^2, \ldots, \alpha^n$ は 1 次従属ゆえ，いずれかは 0 でない $c_0, c_1, c_2, \ldots, c_n \in K$ が存在して

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_n\alpha^n = 0.$$

よって $\alpha$ は $K$ 上代数的で，$L/K$ は代数的拡大ということになる． □

**命題 21.** $K$ を体，$\alpha$ を $K$ の拡大体 $L$ の元で $K$ 上代数的とする．このとき次の性質をもつ既約でモニック[14]な多項式 $m \in K[x]$ が一意的に存在する：
$f \in K[x]$ は $m$ が $f$ を割りきるときに限り $f(\alpha) = 0$ となる．

*Proof.* $I = \{f \in K[x] \mid f(\alpha) = 0\}$ とおくと $I$ は $K[x]$ のゼロでないイデアルで定理 3 によりある $m \in K[x]$ が存在して $I = (m)$．必要なら最高次の係数で割ることで $m$ はモニックとしてよい．$f \in K[x]$ はこの $m$ が $f$ を割りきるときに限り $f(\alpha) = 0$ となる．

$m = gh$ $(g, h \in K[x])$ とすると，$0 = m(\alpha) = g(\alpha)\,h(\alpha)$ で $g(\alpha)$，$h(\alpha)$ のいずれかは 0 である．$g(\alpha) = 0$ であれば $m$ は $g$ を割り切り，$h(\alpha) = 0$ であれば $m$ は $h$ を割り切る．よって $m$ はより低次の 2 つの多項式の積とはならないので $K$ 上で既約ということになる[15]．

もしも $m'$ も条件を満たすとするとモニックな $m$ がモニックな $m'$ を割り切るので $m = m'$ となり，多項式 $m$ は一意的である． □

この命題中の $m$ を $\alpha$ の $K$ 上の **最小多項式** とよび $\mathrm{Irr}(\alpha, K)$ で表す[16]．

$L/K$ を体の拡大，$S \subset L$ とするとき，$K \cup S$ を含む $L$ の最小の部分体を $K$ に $S$ を **添加** してえられる体とよび $K(S)$ で表示する．

$K(\{\alpha_1, \ldots, \alpha_k\})$ は $K(\alpha_1, \ldots, \alpha_k)$ とかく．拡大 $L/K$ はある $L$ の元 $\alpha$ が存在して $L = K(\alpha)$ となっているとき **単純拡大** とよび，$\alpha$ をこのときの **原始元** とよぶ．

**定理 5.** 単純拡大 $K(\alpha)/K$ が有限次であることと $\alpha$ が $K$ 上代数的であることは同値で，このとき $[K(\alpha) : K] = \deg \mathrm{Irr}(\alpha, K)$.

*Proof.* $\deg \mathrm{Irr}(\alpha, K) = n$ とする．$K(\alpha)/K$ が有限次とすると命題 20 より $\alpha$ は $K$ 上代数的となる．

[14] 最高次の係数が 1 であること．
[15] $g$ も $h$ も 0 でないことに注意する．
[16] Irr は 既約 の英語 Irreducible の略．

逆に $\alpha$ は $K$ 上代数的とする．$K[\alpha]=\{f(\alpha)\mid f\in K[x]\}$ とする．写像

$$\phi : K[x] \longrightarrow K[\alpha] \quad , \quad f(x) \longmapsto f(\alpha)$$

は全射準同形で $\alpha$ の $K$ 上の最小多項式 $m$ について $\operatorname{Ker}\phi=(m)$ となっている．よって $K[\alpha]\cong K[x]/(m)$ で $m$ の既約性から $K[\alpha]$ は体であり $K[\alpha]=K(\alpha)$ となる．

$K(\alpha)=K[\alpha]$ の元 $\theta$ はある $f\in K[x]$ が存在して $\theta=f(\alpha)$ であり，$f$ を $m$ で割ると $f=mq+f_0$，$\deg f_0<n$．よって，$\theta=f(\alpha)=m(\alpha)\,q(\alpha)+f_0(\alpha)=f_0(\alpha)$．もしも $n-1$ 次以下の異なる $f_0$，$g_0\in K[x]$ に対して $f_0(\alpha)=g_0(\alpha)$ であれば $\alpha$ が $n-1$ 次以下の 0 でない多項式 $f_0-g_0$ の根となり不合理である．よって，$1,\alpha,\ldots,\alpha^{n-1}$ は $K(\alpha)$ の $K$ 上の基底で拡大 $K(\alpha)/K$ は有限次拡大である． □

**系 2.** 拡大 $L/K$ が有限次であるための必要十分条件は $L$ の有限部分集合 $\{\alpha_1,\ldots,\alpha_k\}$ で $\alpha_i$（$1\le i\le k$）が $K$ 上代数的かつ $L=K(\alpha_1,\ldots,\alpha_k)$ となるのが存在することである．

*Proof.* 拡大 $L/K$ が有限次とすると，代数的拡大で，$L$ の $K$ 上の基底を $\alpha_1,\ldots,\alpha_k$ とすると各 $\alpha_i$（$1\le i\le k$）は $K$ 上代数的で $L=K(\alpha_1,\ldots,\alpha_k)$ となっている．

逆に $L$ の有限部分集合 $\{\alpha_1,\ldots,\alpha_k\}$ で $\alpha_i$（$1\le i\le k$）が $K$ 上代数的かつ $L=K(\alpha_1,\ldots,\alpha_k)$ となるのが存在したとする．$K_i=K(\alpha_1,\ldots,\alpha_i)$ $(1\le i\le k)$ とすると，$K_i=K_{i-1}(\alpha_i)$ $(2\le i\le k)$ であり，$\alpha_i$ は $K_{i-1}$ 上代数的である．よって，$K_i/K_{i-1}$ は各 $i$ に対して有限次拡大であり，タワー公式より $L/K$ は有限次拡大である． □

$L/K$ を体の拡大，$f\in K[x]$ とする．$f$ が定数であるかもしくは $\alpha_1,\ldots,\alpha_n\in L$ が存在して

$$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$$

となるとき $f$ は $L$ 上で **分解する** とよばれる（c は最高次の係数）．$K$ を含む $L$ の真部分体上では分解しないとき $L$ を $K$ 上の $f$ の（最小）**分解体** とよぶ．

**定理 6 (クロネッカーの定理).** $K$ を体，$f\in K[x]$ を定数でない多項式とすると，$K$ のある拡大体 $L$ と $L$ の元 $\alpha$ で $f(\alpha)=0$ となるのが存在する．

*Proof.* $g$ を $f$ の既約因子，$L=K[x]/(g)$ とする．$g$ が既約なので $L$ は体である．

写像 $i : K\longrightarrow L$ を $i(a)=a+(g)$ で定めると，$i$ は体の準同形で $\operatorname{Ker} i=(g)\cap K=\{0\}$ より $i$ は単射である．この $i$ により $K$ を $L$ の部分体とみなし $\alpha=x+(g)$ とすると，$g(\alpha)=0$ で，$g$ は $f$ の因子であるから $f(\alpha)=0$ となる． □

**系 3.** $K$ を体とするとき任意の $f\in K[x]$ に対して $K$ 上の $f$ の分解体が存在する．

$L/K$ と $M/K$ を体の拡大とする．準同形 $\theta : L\longrightarrow M$ が $\theta(a)=a$ $(a\in K)$ であるとき $\theta$ を $K$ **準同形** という．$K$ **同形**，$K$ **自己同形** などが同様に定義される．

**定理 7.** $K_1$, $K_2$ を体，$\sigma : K_1\longrightarrow K_2$ を同形写像とする．$f\in K_1[x]$ で $L_1$ と $L_2$ をそれぞれ $f$ と $\sigma_*(f)$ の分解体とすると $\sigma : K_1\longrightarrow K_2$ は同形 $\tau : L_1\longrightarrow L_2$ に拡張できる．

*Proof.* $[L_1:K_1]$ についての帰納法で示す．$[L_1:K_1]=1$ であれば自明に成り立つ．$[L_1:K_1]>1$ とし，拡大次数がそれより小さい場合は成り立つと仮定する．$L_1\setminus K_1$ 内の $f$ の根 $\alpha$ をえらび，$m=\operatorname{Irr}(\alpha,K_1)$ とする．$m$ は $f$ を割り切るので $\sigma_*(m)$ は $\sigma_*(f)$ を割り切る．よって $\sigma_*(m)$ は $L_2$ 上で分解する．また $\sigma_*(m)$ は既約である．$\sigma_*(m)$ の根 $\beta$ をえらぶと

$$K_1(\alpha)\cong K_1[x]/(m)\cong K_2[x]/(\sigma_*(m))\cong K_2(\beta)$$

$$g(\alpha) \mapsto g + (m) \mapsto \sigma_*(g) + (\sigma_*(m)) \mapsto \sigma_*(g)(\beta)$$

を合成することで $g(\alpha)$ を $\sigma_*(g)(\beta)$ に写す同形 $\phi$ がえられ，これは $\sigma$ の拡張となっている．

$L_1$ と $L_2$ はそれぞれ $f$ と $\sigma_*(f)$ の $K_1(\alpha)$ と $K_2(\beta)$ 上の分解体で，$[L_1 : K_1(\alpha)] < [L_1 : K_1]$ である．帰納法の仮定から $\phi$ の拡張である $\tau : L_1 \longrightarrow L_2$ が存在し，この $\tau$ が求める $\sigma$ の拡張となる． □

**系 4.** 体 $K$ に係数をもつ多項式のどの 2 つの分解体も $K$ 同形である．

*Proof.* 定理 7 で $K_1 = K_2 = K$，$\sigma = id_K$ とすれば示される． □

**系 5.** $L$ をある $K$ 係数の多項式の $K$ 上の分解体，$\alpha, \beta$ は $L$ の元とする．このとき，$\alpha$ を $\beta$ に写す $L$ の $K$ 自己同形が存在する $\Leftrightarrow \mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$.

*Proof.* $\alpha$ を $\beta$ に写す $L$ の $K$ 自己同形 $\sigma$ が存在したとする．任意の $h \in K[x]$ に対して $\sigma(h(\alpha)) = h(\sigma(\alpha)) = h(\beta)$ が成り立つから $h(\alpha) = 0$ と $h(\beta) = 0$ は同値である．したがって，$\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$ でなければならない．

逆に $\alpha$ と $\beta$ を $K$ 上の最小多項式が一致する $L$ の元とする．$K[x]$ のかってな元 $h$ に対して $h(\alpha)$ を $h(\beta)$ に写す $K$ 同形 $\phi : K(\alpha) \longrightarrow K(\beta)$ が定まり，$\phi(\alpha) = \beta$ を満たしている．

$L$ は $K(\alpha)$ 上かつ $K(\beta)$ 上の $f$ の分解体でもあるから，定理 7 より $\phi$ は $\alpha$ を $\beta$ に写す $L$ の $K$ 自己同形に拡張できることになる． □

## 4 ガロア理論

拡大 $L/K$ は $L$ の中に少なくともひとつ根をもつ $K[x]$ の任意の既約多項式が $L$ 上で分解するとき **正規拡大** とよばれる[17].

**定理 8.** 体 $K$ の拡大体 $L$ について，$L$ はある $K$ 係数の多項式の $K$ 上の分解体である $\Leftrightarrow$ 拡大 $L/K$ は有限次かつ正規.

*Proof.* $L/K$ が有限次かつ正規とする．$L$ の代数的元 $\alpha_1, \alpha_2, \ldots, \alpha_n$ で $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ となるのが存在する．$m_j = \mathrm{Irr}(\alpha_j, K)$ とおき，$f = m_1 m_2 \cdots m_n$ とする．$m_j$ は $L$ 上で分解するから $f$ も $L$ 上で分解する．$L$ は $f$ のすべての根を $K$ に添加してえられるので，$L$ は $K$ 上の $f$ の分解体である．

逆に $L$ はある $K$ 係数の多項式の $K$ 上の分解体とする．$L$ は $f$ の根を $K$ に添加してえられるので拡大 $L/K$ は有限次である．

$g \in K[x]$ を既約，$M$ を多項式 $fg$ の $L$ 上の分解体とする．すると $L \subset M$ で多項式 $f$ と $g$ は $M$ 上で分解する．$\beta$，$\gamma$ を $M$ における $g$ の根とする．$f$ は $L(\beta)$ および $L(\gamma)$ 上で分解する．更に $f$ が $K(\beta)$ を含む $M$ の部分体上で分解するならその部分体は $L$ を含んでいなければならないので $L(\beta)$ を含んでいることになる．よって $L(\beta)$ は $f$ の $K(\beta)$ 上の分解体である．同様にして $L(\gamma)$ は $f$ の $K(\gamma)$ 上の分解体である．

$K$ 係数のかってな多項式 $h$ に対して $h(\beta)$ を $h(\gamma)$ に写す $K$ 同形 $\sigma : K(\beta) \longrightarrow K(\gamma)$ が存在する．この $K$ 同形 $\sigma$ は $K$ 同形 $\tau : L(\beta) \longrightarrow L(\gamma)$ に拡張できる．よって $[L(\beta) : K] = [L(\gamma) : K]$．ここで $[L(\beta) : K] = [L(\beta) : L][L : K]$，$[L(\gamma) : K] = [L(\gamma) : L][L : K]$ であるから $[L(\beta) : L] = [L(\gamma) : L]$．とくに $\beta \in L$ と $\gamma \in L$ は同値であり，拡大 $L/K$ は正規である． □

体 $K$ 係数の多項式 $f = \sum_{i=0}^{n} c_i x^i$ に対して $f$ の（形式的）**導多項式** $Df$ を $(Df)(x) = \sum_{i=1}^{n} i c_i x^{i-1}$ と定める．$D$ は **微分作用素** とよぶ.

[17] かってな $L$ の元 $\alpha$ に対して $\mathrm{Irr}(\alpha, K)$ が $L$ 上で分解することと同値である.

**命題 22.** 次の公式が成立する.

(i) $D(f+g) = Df + Dg$, $D(fg) = (Df)g + f(Dg)$, $D(kf) = k(Df)$ $(k \in K)$.

(ii) $D(f^n) = nf^{n-1}(Df)$ $(n \geq 2)$.

*Proof.* $D(f+g) = Df + Dg$ と $D(kf) = k(Df)$ は容易に示される. よって $D$ は線形であり, $D(fg) = (Df)g + f(Dg)$ は $f = x^r$, $g = x^s$ として示せばよい. $D(f^n) = nf^{n-1}(Df)$ は $D(fg) = (Df)g + f(Dg)$ から帰納的に導ける. □

$L/K$ を体の拡大, $f \in K[x]$ とする. $L$ の元 $\alpha$ は $(x-\alpha)^2$ が $f$ を割り切るとき **重根** という.

**命題 23.** 体 $K$ 係数の多項式 $f$ に対して, $f$ が $K$ 上の分解体において重根をもつことは, $K[x]$ 内で $f$ と $Df$ を割り切る $K$ 係数の定数でない多項式が存在することと同値である.

*Proof.* $f \in K[x]$ がある分解体 $L$ において重根 $\alpha$ をもつとすると, ある $h \in L[x]$ が存在して $f = (x-\alpha)^2 h$ となり $Df = 2(x-\alpha)h + (x-\alpha)^2 Dh$. よって $(Df)(\alpha) = 0$ となり, $\mathrm{Irr}(\alpha, K)$ は $K$ 係数の定数でない多項式で $f$ と $Df$ を割り切る.

逆に $f \in K[x]$ はある定数でない $g \in K[x]$ によって $f$ と $Df$ が割り切れるとする. $L$ を $K$ 上の $f$ の分解体とすると, $g$ は $f$ の因子であるから $g$ も $L$ 上で分解する. $\alpha \in L$ を $g$ の根とすると $\alpha$ は $f$ の根でもあるからある $e \in L[x]$ が存在して $f = (x-\alpha)e$ となる. 微分すると $Df = e + (x-\alpha)De$. $g(\alpha) = 0$ で $g$ は $K[x]$ において $Df$ を割り切ることから $Df(\alpha) = 0$ で, $e(\alpha) = 0$ を得る. よってある $h \in L[x]$ が存在して $e = (x-\alpha)h$. したがって $f = (x-\alpha)^2 h$ となり, $f$ は分解体 $L$ 内で重根をもつ. □

$K$ を体とするとき, 既約多項式 $f \in K[x]$ は $K$ 上の分解体において重根をもたないとき $K$ 上で **分離的** とよばれる. 多項式 $f \in K[x]$ はどの既約因子も $K$ 上で分離的なとき $K$ 上で **分離的** とよぶ.

**系 6.** 体 $K$ 係数の既約多項式 $f$ に対して, $f$ が非分離的であることは $Df = 0$ と同値である.

*Proof.* $f \in K[x]$ は非分離的かつ既約な多項式とする. $f$ は分解体において重根をもち, $K[x]$ 内で $f$ と $Df$ を割り切る $K$ 係数の定数でない多項式 $g$ が存在する. $f$ は既約ゆえ, ある 0 でない $c \in K$ により $g = cf$ となり $f \mid Df$. このことと $\deg Df < \deg f$ から $Df = 0$ でなければならないことになる.

逆に $Df = 0$ と仮定する. $f$ は $f$ と $Df$ を割り切るので, $f$ は分解体において重根をもつことになり非分離的である. □

代数的拡大 $L/K$ は $L$ の各元 $\alpha$ についてその最小多項式 $\mathrm{Irr}(\alpha, K)$ が $K$ 上で分離的なとき **分離的拡大** とよばれる.

**系 7.** 標数 0 の体 $K$ を係数とする多項式は $K$ 上で分離的で, どの体拡大 $L/K$ も分離的である.

*Proof.* $\mathrm{char}\, K = 0$ であることから $f \in K[x]$ について $Df = 0$ であることと定数多項式であることは同値である. よって系 6 により成り立つ. □

**補題 1.** 標数 $p$ が正の体 $K$ においては任意の $x, y \in K$ に対して $(x+y)^p = x^p + y^p$, $(xy)^p = x^p y^p$ が成り立ち, 写像 $K \ni x \mapsto x^p \in K$ は単射準同形である[18].

[18] この単射準同形は **フロベニウス準同形** とよばれる. $K$ が有限体であればフロベニウス準同形は $K$ の自己同形である.

*Proof.* $(xy)^p = x^p y^p$ は $K$ の可換性からただちにえられる．2 項展開の公式 $(x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}$ が成り立ち，$0 < j < p$ のとき $p \mid \binom{p}{j}$ であることから $(x+y)^p = x^p + y^p$ をえる．また，$1^p = 1$ も成り立つので写像 $K \ni x \mapsto x^p \in K$ は準同形である．$x \neq y$ とすると $x^p - y^p = (x-y)^p \neq 0$ より $x^p \neq y^p$．よって写像 $K \ni x \mapsto x^p \in K$ は単射である[19]． □

**定理 9.** $p$ を素数，$n$ を正の整数とするとき，体 $K$ が $p^n$ 個の元をもつことと $K$ が部分体 $\mathbb{F}_p$ 上の多項式 $x^{p^n} - x$ の分解体であることは同値である．ここで $\mathbb{F}_p$ は $\mathbb{Z}_p$ と同形な体である．

*Proof.* $q = p^n$ として，体 $K$ は $q$ 個の元をもつとする．$K^\times = K - \{0\}$ は乗法に関して位数 $q-1$ の群をなすから $\alpha \in K^\times$ に対して $\alpha^{q-1} = 1$．よって任意の $\alpha \in K$ に対して $\alpha^q = \alpha$ となる．したがって $K$ のすべての元は $x^q - x$ の根である．$x^q - x$ の次数が $q$ で $K$ が $q$ 個の元をもつことから $x^q - x$ は $K$ 上で分解する．また，$x^q - x$ は $K$ の真部分体上では分解しないので $K$ は $x^q - x$ の分解体である．

逆に，$f = x^q - x, q = p^n$ として，$K$ は $\mathbb{F}_p$ 上の $f$ の分解体とする．写像 $\sigma : K \ni \alpha \mapsto \alpha^q \in K$ は $K$ のフロベニウス準同形を $n$ 回合成してえられるので単射準同形である．また，$K$ の元 $\alpha$ が $f$ の根であることと $\sigma(\alpha) = \alpha$ は同値である．このことから $f$ の根の全体は $K$ の部分体をなし，$K$ が分解体であることから $K$ と一致する．$q$ が $\mathbb{F}_p$ の標数 $p$ の倍数であることから $Df = qx^{q-1} - 1 = -1$ で，命題 23 により $f$ のどの根も相異なる．よって $f$ は $q$ 個の根をもち，$K$ は $q$ 個の元をもつことになる． □

$K$ を標数 $p$ の有限体，$n = [K : \mathbb{F}_p]$ とすると $\sharp K = p^n$ であるから，系 3 と系 4 により次の系がえられる．

**系 8.** 素数 $p$ と正の整数 $n$ に対して位数 $p^n$ の有限体 $\mathbf{GF}(p^n)$ が存在する[20]．2 つの有限体が同形であるための必要十分条件は位数が等しいことである．

正の整数 $n$ に対して $\varphi(n)$ を $0 \leq x < n$ で $n$ と互いに素である整数 $x$ の個数とする[21]．

**補題 2.** 正の整数 $n$ に対して $\sum_{d \mid n} \varphi(d) = n$ が成立する．

*Proof.* $d \mid n$ のとき 1 から $n$ までの整数の中に最大公約数 $(x, n)$ が $d$ となる $x$ は $\varphi(n/d)$ 個ある．よって $x = 1, 2, \ldots, n$ を $(x, n) = d$ により分類すると，$n$ の約数を 1 から順に $1, d_1, d_2, \ldots, n$ として，$d = 1$ で決まるのは $\varphi(n)$ 個，$d = d_1$ で決まるのは $\varphi(n/d_1)$ 個，$\cdots$，$d = n$ で決まるのは $\varphi(1) = 1$ 個である．ゆえに $\varphi(n) + \varphi(n/d_1) + \varphi(n/d_2) + \cdots + \varphi(1) = n$.

$n, n/d_1, n/d_2, \cdots, 1$ は $1, d_1, d_2, \cdots, n$ の逆順の数列で全体としては一致している． □

**定理 10.** 体の非ゼロ元全体のなす乗法群の有限部分群 $G$ は巡回群である．

*Proof.* $n$ を群 $G$ の位数とする．ラグランジュの定理より $G$ の各元の位数は $n$ の約数である．$n$ の約数 $d$ に対して位数が $d$ である $G$ の元の個数を $\psi(d)$ で表すことにする．$\sum_{d \mid n} \psi(d) = n$ である．

$n$ の約数 $d$ について，$g$ を位数 $d$ の $G$ の元とする．$1, g, g^2, \ldots, g^{d-1}$ は $G$ の異なる元で，いずれも次数が $d$ の多項式 $x^d - 1$ の根となっている．よって $x^d = 1$ を満たす $G$ の元 $x$ は $0 \leq k < d$ である整数 $k$ が一意的に決まって $x = g^k$ ということになる．$k$ と $d$ が互いに素であれば，$\left(g^k\right)^m = 1$ であるとき $d \mid km$ であるから $d \mid m$ となり，$g^k$ の位

[19] 核が $\{0\}$ だから単射といってもよい．
[20] 体 $\mathbf{GF}(p^n)$ は位数 $p^n$ の **ガロア体** とよばれる．
[21] 関数 $\varphi$ は **オイラー関数** とよばれる．

数は $d$ であることがわかる．逆に $g^k$ の位数が $d$ とすると，$e$ を $k$ と $d$ の公約数として $\left(g^k\right)^{d/e} = g^{d(k/e)} = 1$ より $e = 1$ となるので，$d$ と $k$ は互いに素である．したがって，位数が $d$ の $G$ の元 $g$ が存在すれば，位数が $d$ である $G$ の元の全体は $d$ と互いに素な $0 \leq k < d$ である整数 $k$ に対する $g^k$ の全体と一致する．このことから $\psi(d) > 0$ のとき $\psi(d) = \varphi(d)$ である．$n$ の各約数 $d$ について $0 \leq \psi(d) \leq \varphi(d)$ であるが，$\sum_{d|n} \psi(d)$ も $\sum_{d|n} \varphi(d)$ も $n$ なので，$n$ の各約数 $d$ について $\psi(d) = \varphi(d)$ である．とくに $\psi(n) = \varphi(n) \geq 1$ であるから，$G$ は位数が $n$ の元をもつことになり巡回群である． □

**系 9.** 有限体の非ゼロ元全体のなす乗法群は巡回群である．

**定理 11 (原始元定理).** 有限次分離的拡大は単純拡大である．

*Proof.* $L/K$ を有限次分離的拡大とする．$K$ を有限体とすると，$L$ は $K$ 上有限次のベクトル空間なので $L$ も有限体である．よって $L \setminus \{0\}$ は乗法により巡回群で生成元 $\theta$ をもつ．よって $L = K(\theta)$ となり $L/K$ は単純拡大である．

次に $L = K(\beta, \gamma)$ で，$K$ は無限体，$\beta$ と $\gamma$ は $K$ 上代数的，拡大 $L/K$ は分離的とする．$f = \mathrm{Irr}(\beta, K)$，$g = \mathrm{Irr}(\gamma, K)$ として，$N$ を積 $fg$ の分解体とする．このとき $f$ も $g$ も $N$ 上で分解する，$\beta_1, \beta_2, \ldots, \beta_q$ を $N$ における $f$ の根，$\gamma_1, \gamma_2, \ldots, \gamma_r$ を $N$ における $g$ の根，$\beta_1 = \beta$，$\gamma_1 = \gamma$ とする．$L/K$ の分離性から $\gamma_1, \gamma_2, \ldots, \gamma_r$ はお互いに異なる．

$\sharp K = \infty$ であることからどの $i$，$j(\neq 1)$ に対しても $c \neq \frac{\beta_i - \beta}{\gamma - \gamma_j}$ であるような $c \in K$ がえらべる．$\theta = \beta + c\gamma$ として $h(x) = f(\theta - cx)$ とおく．すると $h$ は $K(\theta)$ 係数の不定元 $x$ の多項式で，$g$ と $h$ の共通根は $\gamma$ のみである．したがって $K(\theta)[x]$ の中での $g$ と $h$ の最大公約因子は $x - \gamma$ で，$\gamma \in K(\theta)$ である．すると $\beta = \theta - c\gamma$ で $c \in K$ であることから $\beta \in K(\theta)$ となる．よって $L = K(\theta)$ となる．

あとは $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ ($K$ は無限体，$\alpha_1, \alpha_2, \ldots, \alpha_m$ は $K$ 上代数的) について $L/K$ が分離的なら単純であることは $m$ による帰納法で示される． □

体 $L$ の自己同形全体は写像の合成により群をなす．この群を $L$ の（全）**自己同形群** とよび $\mathrm{Aut}(L)$ とかく．

拡大 $L/K$ に対して $K$ 自己同形全体は $\mathrm{Aut}(L)$ の部分群である．この部分群を拡大 $L/K$ の **ガロア群** とよび $\mathrm{Gal}(L/K)$ で表す．

**命題 24.** 拡大 $L/K$ が有限次分離的ならば $\sharp\mathrm{Gal}(L/K) \leq [L : K]$.

*Proof.* 原始元定理（定理 11）より $L$ の元 $\alpha$ が存在して $L = K(\alpha)$ である．$\lambda$ を $L$ の元とすると，ある $K$ 係数多項式 $g$ が存在して $\lambda = g(\alpha)$．$g$ の係数は $\sigma$ で不変なので任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(\lambda) = g(\sigma(\alpha))$ で $\mathrm{Gal}(L/K)$ に属する各自己同形 $\sigma$ は $\sigma(\alpha)$ が与えられると一意的に定まることになる．

$f = \mathrm{Irr}(\alpha, K)$ とする．$f$ の係数は $K$ に属し $\sigma$ により不変であるから $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ で $\sigma(\alpha)$ は $f$ の根である．よって $\sharp\mathrm{Gal}(L/K)$ は $L$ に属する $f$ の根の個数以下で，したがって $\deg f$ 以下となる．定理 5 より $\deg f = [L : K]$ であるから $\sharp\mathrm{Gal}(L/K) \leq [L : K]$ となる． □

$\mathrm{Aut}(L)$ の部分群 $G$ に対して $L^G = \{a \in L \mid \sigma(a) = a (\sigma \in G)\}$ は $L$ の部分体で $L$ の $G$ による **固定体** とよぶ．

**命題 25.** $L$ を体，$G$ を $\mathrm{Aut}(L)$ の有限部分群，$K = L^G$ とすると，$L$ の各元 $\alpha$ は $K$ 上代数的で，$\mathrm{Irr}(\alpha, K)$ は

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

となる．但しここで，$\alpha_1, \alpha_2, \ldots, \alpha_k$ は $L$ 上の $G$ の作用による $\alpha$ の軌道[22]の元で相異なるものの全体とする．

*Proof.* $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ とおくと，$G$ に属する各自己同形は $\alpha_1, \alpha_2, \ldots, \alpha_k$ を置換し因子を置換することになるから $f$ は $G$ の作用により不変である．よって $f$ の係数は $K$ に属し $\alpha$ は $f$ の根であるから $K$ 上代数的である．

$f$ のかってな根 $\alpha_i$ に対して $\alpha_i = \sigma(\alpha)$ となる $\sigma \in G$ が存在する．したがって $g \in K[x]$ について $g(\alpha) = 0$ とすると，$g$ の係数は $\sigma$ により不変であるから，$g(\alpha_i) = \sigma(g(\alpha)) = 0$ である．よって $f$ は $g$ を割り切るので $f = \mathrm{Irr}(\alpha, K)$ である． □

有限次，正規，かつ分離的な体の拡大を（有限次）**ガロア拡大** という．

**定理 12.** $L$ を体，$G$ を $\mathrm{Aut}(L)$ の有限部分群，$K = L^G$ とすると，拡大 $L/K$ はガロア拡大であり $G = \mathrm{Gal}(L/K)$，$\sharp G = [L : K]$ となっている．

*Proof.* 命題 25 より，各 $\alpha \in L$ について $\mathrm{Irr}(\alpha, K)$ は $L$ 上で分解し重根をもたない．したがって拡大 $L/K$ は正規かつ分離的である．

M を $[M : K] < \infty$ であるような $L/K$ の中間体とする．拡大 $L/K$ が分離的なので $M/K$ も分離的であり，原始元定理より $M/K$ は単純拡大で，ある $\alpha \in L$ が存在して $M = K(\alpha)$ となる．すると $[M : K] = \deg \mathrm{Irr}(\alpha, K)$ であり，命題 25 より $[M : K]$ は $L$ 上の $G$ の作用による $\alpha$ の軌道の元の数と一致する．よって $[M : K]$ は $\sharp G$ の約数である．

$M$ を $[M : K] < \infty$ であるような $L/K$ の中間体の内で $[M : K]$ が最大であるように選ぶ．もしも $\lambda \in L$ であれば $\lambda$ は $K$ 上代数的で $[M(\lambda) : M] < \infty$ となり，タワー公式により $[M(\lambda) : K] < \infty$ で $[M(\lambda) : K] = [M(\lambda) : M][M : K]$ となる．$M$ の選び方から $[M(\lambda) : K] = [M : K]$ で $[M(\lambda) : M] = 1$．よって $M = L$．したがって $L/K$ は有限次拡大でもあるから結局ガロア拡大であり，$[L : K]$ は $\sharp G$ の約数である．

また，$\sharp\mathrm{Gal}(L/K) \leq [L : K] \leq \sharp G \leq \sharp\mathrm{Gal}(L/K)$ より $G = \mathrm{Gal}(L/K)$，$\sharp G = [L : K]$ を得る． □

**定理 13.** 有限次拡大 $L/K$ に対して $\sharp\mathrm{Gal}(L/K)$ は $[L : K]$ の約数である．また，$\mathrm{Gal}(L/K) = [L : K]$ であるための必要十分条件は $L/K$ がガロア拡大であることであり，このとき $K = L^{\mathrm{Gal}(L/K)}$ となっている．

*Proof.* $M = L^{\mathrm{Gal}(L/K)}$ とする．定理 12 より $L/M$ はガロア拡大で $\sharp\mathrm{Gal}(L/K) = [L : M]$ である．$[L : K] = [L : M][M : K]$ なので $\sharp\mathrm{Gal}(L/K)$ は $[L : K]$ の約数である．もしも $\sharp\mathrm{Gal}(L/K) = [L : K]$ であれば $M = K$ となるので $L/K$ はガロア拡大で $K = L^{\mathrm{Gal}(L/K)}$ である．

逆に $L/K$ をガロア拡大とする．原始元定理より，ある $\theta \in L$ が存在して $L = K(\theta)$ である．$f = \mathrm{Irr}(\theta, K), \deg f = n$ とする．$f$ は既約で $L/K$ は正規拡大であることから $f$ は $L$ 上で分解する．$L$ における $f$ の根を $\theta_1, \theta_2, \ldots, \theta_n$，$\theta_1 = \theta$，とする．$\sigma$ が $L$ の $K$ 自己同形とすると，$f$ のどの係数も $K$ に属し $\sigma$ により不動であるから，$f(\sigma(\theta)) = \sigma(f(\theta)) = 0$. よって，ある $j$ について $\sigma(\theta) = \theta_j$ である．$f$ の各根 $\theta_j$ に対して $\sigma_j(\theta) = \theta_j$ となるような $L$ の $K$ 自己同形 $\sigma_j$ が丁度ひとつ存在することを示す.

$g(x), h(x) \in K[x]$ について $g(\theta) = h(\theta)$ とする．$g - h$ は最小多項式 $f$ で割り切れるので，$f$ の任意の根 $\theta_j$ に対して $g(\theta_j) = h(\theta_j)$ となる．$L = K(\theta)$ より $L$ の元はある $g \in K[x]$ が存在して $g(\theta)$ というカタチをしているので，任意の $g \in K[x]$ に対して $\sigma_j(g(\theta)) = g(\theta_j)$ である写像 $\sigma_j : L \longrightarrow L$ が定義できることになる。定義により $\sigma_j$ は $K$ を固定し $\theta$ を $\theta_j$ に写す $L$ の唯一の自己同形である．

[22] $\{\sigma(\alpha) \mid \sigma \in G\}$ を指す.

$f$ が既約で拡大 $L/K$ が分離的であることから $L$ において $f$ は重根をもたない．また，各根は $\mathrm{Gal}(L/K)$ の丁度ひとつの元を決定するので $\sharp\mathrm{Gal}(L/K)$ は $f$ の根の総数と一致し，$\sharp\mathrm{Gal}(L/K) = \deg f$ であることになる．よって定理5より $\sharp\mathrm{Gal}(L/K) = [L:K]$ である． □

**命題 26.** $M$ を $L/K$ の中間体とする．$L/K$ がガロア拡大ならば $L/M$ もガロア拡大である．更に $M/K$ が正規であれば $M/K$ もガロア拡大である．

*Proof.* $\alpha \in L$, $f_K = \mathrm{Irr}(\alpha, K)$, $f_M = \mathrm{Irr}(\alpha, M)$ とする．$f_K$ は $K$ 上既約で $L/K$ は正規なので $f_K$ は $L$ 上で分解する．また，$L/K$ が分離的であることから $L$ において $f_K$ は重根をもたない．$f_K(\alpha) = 0$ で $f_K$ の係数が $M$ に属することから $f_M$ は $f_K$ を割り切ることになり，$f_M$ も $L$ 上で分解し重根をもたない．よって，有限次拡大 $L/M$ が正規かつ分離的ゆえガロア拡大である．

また，$L/K$ が分離的であることから有限次拡大 $M/K$ も分離的なので, もしも $M/K$ が正規拡大ならガロア拡大となる． □

**命題 27.** $L/K$ がガロア拡大，$M$ が $L/K$ の中間体であるとき，拡大 $M/K$ が正規であるための必要十分条件は，任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) = M$ となっていることである．

*Proof.* $\alpha \in M, f = \mathrm{Irr}(\alpha, K)$ とする．$L/K$ がガロア拡大であることから $K = L^{\mathrm{Gal}(L/K)}$ で，多項式 $f$ は $L$ 上で分解し，$f$ の根は $L$ 上の $\mathrm{Gal}(L/K)$ の作用による $\alpha$ の軌道の元たちである．よって $f$ が $M$ 上で分解することとかってな $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(\alpha) \in M$ であることは同値である．$M/K$ が正規であることは $M$ の任意の元の $K$ 上の最小多項式が $M$ 上で分解することと同値であるから，$M/K$ が正規であることとかってな $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) \subset M$ であることが同値となるが，これは任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) = M$ であることと同値である． □

**系 10.** $L/K$ をガロア拡大，$M$ を $L/K$ の中間体とする．拡大 $M/K$ が正規であるとき $L$ の任意の $K$ 自己同形 $\sigma$ の $M$ への制限 $\sigma\,|_M$ は $M$ の $K$ 自己同形である．

**定理 14 (ガロア理論の基本定理).** ガロア拡大 $L/K$ に対して, $L/K$ の中間体 $M$ にガロア群 $\mathrm{Gal}(L/M)$ を対応させ $\mathrm{Gal}(L/K)$ の部分群 $G$ に固定体 $L^G$ を対応させると $L/K$ の中間体 $M$ と $\mathrm{Gal}(L/K)$ の部分群 $G$ は1：1に対応する．更に，$M/K$ が正規拡大であることと $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群であることは同値で，このとき $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ が成立する．

*Proof.* $M$ を $L/K$ の中間体とすると命題26より $L/M$ はガロア拡大であり，求める1：1対応の存在は定理12，定理13からただちに云える．

$L/K$ の中間体 $M$ に対して，命題27より $M/K$ が正規拡大であることと任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) = M$ であることは同値で，$M$ と $\sigma(M)$ はそれぞれ $\mathrm{Gal}(L/M)$ と $\sigma\mathrm{Gal}(L/M)\sigma^{-1}$ による固定体であるから，$M = \sigma(M)$ は $H = \sigma H \sigma^{-1}$ と同値である．したがって，$M/K$ が正規拡大であることと $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群であることは同値である．

$M/K$ は正規拡大とし, 各 $\sigma \in \mathrm{Gal}(L/K)$ に対して $\rho(\sigma)$ を $\sigma\,|_M$ とする．$\rho : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K)$ は群準同形で $\mathrm{Ker}\,\sigma = \mathrm{Gal}(L/M)$ である．$K = M^{\rho(\mathrm{Gal}(L/K))}$ であるから，定理12を拡大 $M/K$ に適用することにより $\rho$ は全射であることがわかる．よって，準同形 $\rho$ は $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ と $\mathrm{Gal}(M/K)$ の同形を導く． □

# 5　方程式論への応用

群 $G$ の部分群の減小列

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{r-1} \supset G_r = (e)$$

は各 $i = 1, 2, \ldots, r$ について $G_{i-1} \triangleright G_i$ となっているとき **正規列** という．各剰余群 $G_{i-1}/G_i$ がアーベル群となっているときは **アーベル**（正規）**列** といい，アーベル列をもつ群を **可解群** という．たとえばアーベル群は可解である．

次の定理はよく知られている．

**定理 15.** $n \geq 5$ の対称群 $S_n$ は可解でない．

体に係数をもつ多項式 $f$ が，$f$ の分解体におけるすべての根が $f$ の係数から加法，減法，乗法，除法，およびべき根に開くという操作を有限回施してえられるとき，$f$ は **べき根により可解** とよぶ．

$f$ を体 $K$ に係数をもつ多項式，$L$ を $K$ 上の $f$ の分解体とするとき，ガロア群 $\mathrm{Gal}(L/K)$ を $K$ 上の $f$ の **ガロア群** といい $\mathrm{Gal}_K(f)$ で表す．

**補題 3.** $f$ を体 $K$ 係数の多項式，$M$ を $K$ の拡大体とすると，$\mathrm{Gal}_M(f)$ は $\mathrm{Gal}_K(f)$ の部分群と同形である．

*Proof.* □

**補題 4.** 体 $K$ 係数の $n$ 次多項式 $f$ に対してそのガロア群 $\mathrm{Gal}_K(f)$ は $n$ 次対称群 $S_n$ の部分群と同形である．

*Proof.* □

**補題 5.** $K$ を体，$p$ を $K$ の標数と等しくない素数とするとき，$K$ のある拡大体における 1 の原始 $p$ 乗根 $\omega$ に対してガロア群 $\mathrm{Gal}\left(K\left(\omega\right)/K\right)$ はアーベル群である．

*Proof.* □

**補題 6.** $K$ を標数が 0 の体，$p$ は素数，$c$ は $K$ の元とする．$M$ を多項式 $x^p - c$ の $K$ 上の分解体とすると，ガロア群 $\mathrm{Gal}(M/K)$ は可解である．

*Proof.* □

**補題 7.** $f$ を標数が 0 の体 $K$ に係数をもつ多項式，$\alpha$ をある素数 $p$ について $\alpha^p \in K$ であるような $K$ の拡大体の元，$K' = K\left(\alpha\right)$ とするとき，$\mathrm{Gal}_K(f)$ が可解であることと $\mathrm{Gal}_{K'}(f)$ が可解であることは同値である．

*Proof.* □

**定理 16.** 標数 0 の体 $K$ に係数をもつ多項式 $f$ に対して，$f$ がべき根により可解ならばそのガロア群 $\mathrm{Gal}_K(f)$ は可解である．

*Proof.* □

**補題 8.** $p$ を素数，$K$ を標数が $p$ と等しくない体，拡大 $L/K$ を拡大次数が $p$ の $K$ のガロア拡大とするとき，多項式 $x^p - 1$ が $K$ 上で分解するならばある $\alpha \in L$ が存在して $L = K\left(\alpha\right)$ かつ $\alpha^p \in K$ となる．

*Proof.* □

**定理 17.** 標数 0 の体 $K$ に係数をもつ多項式 $f$ に対して，ガロア群 $\mathrm{Gal}_K(f)$ が可解ならば $f$ はべき根により可解である．

*Proof.* □

定理 16，定理 17 を一緒にして次を得る．

**定理 18 (ガロアの定理).** $f$ を標数 0 の体 $K$ に係数をもつ多項式とするとき次は同値である．
（1）$f$ はべき根により可解.
（2）$\mathrm{Gal}_K(f)$ は可解群.

**定理 19 (アーベルの定理).** $n$ 次の一般方程式が代数的に解けるための必要十分条件は $n \leq 4$ である．

*Proof.* □

## 6 あとがき（本の紹介など）

比較的読みやすい本を参考文献として掲げておきました．読み物風が好みのひとには [4], [1]，教科書風が好みのひとには [2]，[5]，[3] がオススメです.

更に体論，ガロア理論を勉強したいひとはこれらの本の参考文献を参考にしてください.

## 参考文献


[1] 草場公邦著『ガロワと方程式』（朝倉書店，1989 年）

[2] 松田隆輝著『ガロア理論』（槇書店，1996 年）

[3] 酒井文雄著『環と体の理論』（共立出版，1997 年）

[4] 弥永昌吉著『ガロアの時代 ガロアの数学 第二部 数学篇』（シュプリンガー・フェアラーク東京，2002 年）

[5] 弥永昌吉 有馬哲 浅枝陽著『詳解 代数入門』（東京図書，1990 年）