代数学続論講義ノート

安藤哲哉

注意: 校正をあまりきちんとしていないので，誤植等に注意して利用して下さい．

1. 基礎概念

代数学 II までに習っているはずだが，もう一度，環・整域・体の定義の復習から始める．知っている部分は読まなくてよい．

定義 1.1.(可換環，整域，体, 加群) 集合 R に 2 種類の和 $+$ と積 $\times$ が定義されていて以下 (1) 〜 (3) を満たすとき R を**可換環** (commutative ring) という．ただし，積 $a \times b$ は通号 ab と書き，時に $a \cdot b$ とも書く．

(1) R は和 $+$ について 0 を単位元とするアーベル群である．
(2) R は積について閉じていて，結合法則，交換法則を満たし，1 を単位元とする．つまり，$a, b \in R$ ならば $ab \in R$ で，$(ab)c = a(bc)$, $ab = ba$, $1a = a$ $(\forall a, \forall b, \forall c \in R)$ を満たす．
(3) 分配法則 $(a+b)c = ac + bc$ $(\forall a, \forall b, \forall c \in R)$ を満たす．

以上の定義から，$0a = 0$ (なぜなら $(0a + 0a = (0 + 0)a = 0a)$, $a(b + c) = ab + ac$ が導かれることに注意する．ところで，可換環 R の定義の中で $0 \neq 1$ は仮定しなかったが，もし $0 = 1$ であれば $R = \{0\}$ である．実際，$a \in R$ ならば $a = 1a = 0a = 0$ である．可換環 $\{0\}$ を単に 0 とも書く．

今，R は可換環で $R \neq 0$ とする．$a \in R$ に対し $ab = 1$ を満たす $b \in R$ が存在するとき，この b を $b = a^{-1}$ とか $1/a$ とか $b = \dfrac{1}{a}$ と書き，a の**逆元**という．a が逆元を持つとき a は**可逆** (invertible) 元であるとか，**単元** (unit) であるという．

また，$a \in R$ に対し，$ab = 0$, $b \neq 0$ を満たす $b \in R$ が存在するとき，a は**零因子**とか**ゼロ因子** (zero dividor) であるという．a が零因子でないとき**非零因子**とか**正則元** (regular) という．

環 R において，$\underbrace{1 + 1 + \cdots + 1}_{n\text{ 個}} = 0$ となることがある (後の例 1.2(3) 参照)．この場合，この条件を満たす最小の自然数 n を R の**標数** (characteristic) という．何個 1 を足しても 0 にならないとき，R の標数は 0 であると約束する．

可換環 R が以下の (4), (5) を満たすとき，R は**整域** (integral domain) であるという．

(4) $0 \neq 1$ である．
(5) 0 以外に零因子は存在しない．つまり，$a, b \in R$, $ab = 0$ ならば $a = 0$ または $b = 0$ である．対偶で書けば，$a \neq 0$, $b \neq 0$ ならば $ab \neq 0$ である．

可換環 R が上の (4) と以下の (6) を満たすとき，R は (可換) **体** (field) であるという．

(6) R の 0 でない元は R の中に逆元を持つ．つまり，$0 \neq a \in R$ ならば，$a^{-1} \in R$.

容易にわかるように，体は整域である．

可換環 R の部分集合 $S \subset R$ が和と積について閉じていて，$a \in S$ であるとき，S は R の**部分環**であるという．S が整域のとき S は R の**部分整域**，S が体のとき S は R の**部分体**であるという．

R が可換環，M は加法 $+$ についてのアーベル群で，任意の $a \in R$ と $x \in M$ に対してスカラー倍とか R の作用とか呼ばれる演算 ax が定義されていて，$ax \in M$ を満たすとする．さらに，任意の a, $b \in R$ と $x, y \in M$ に対して，

(7) (分配法則) $a(x + y) = ax + ay$, $(a + b)x = ax + bx$.
(8) (結合法則) $(ab)x = a(bx)$.
(9) (1 の自明な作用) $1x = x$. ただし 1 は R の単位元.

を満たすとき，M は R-**加群**であるという．K が体のとき，K-加群を K-**ベクトル空間**ともいう．

例 1.2. (1) 整数全体の集合 $\mathbb{Z}$ は体でない整域である．

(2) 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ はいずれも体である．

(3) 自然数 n を法とする剰余系 $\mathbb{Z}/n\mathbb{Z}$ は可換環である．n が合成数 (2 つ以上の素数の積) であるとき $\mathbb{Z}/n\mathbb{Z}$ は整域でない可換環である．実際 $n = pq$ $(p \geqq 2, q \geqq 2)$ のとき，その n を法とする剰余類は，$\overline{0} = \overline{n} = \overline{p}\,\overline{q}$, $\overline{0} \neq \overline{p}$, $\overline{0} \neq \overline{q}$ である．

定義 1.3.(準同型写像) R, S は可換環とする．写像 $f\colon R \to S$ が以下の (1), (2) を満たすとき，f は (可換環としての) **準同型**写像 (homomorphism) であるという．
(1) $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ $(a, b \in R)$
(2) $f(1_R) = 1_S$

上の定義から，$f(0_R) = 0_S$ も導かれる．また，$a \in R$ が R の可逆元ならば $f(a^{-1}) = f(a)^{-1}$ なので，$f(a)$ は S の可逆元である．$f\colon R \to S$ が準同型写像で全単射であると，逆写像 $f^{-1}\colon S \to R$ も準同型写像になる．このとき，$f\colon R \to S$ は**同型写像**であるといい，$f\colon R \xrightarrow{\cong} S$ などと書く．同型写像 $f\colon R \to S$ が存在するとき R と S は**同型**であるといい，$R \cong S$ などと書く．この用語は R, S が体の場合にも，そのまま用いる．

K, L が体で，$f\colon K \to L$ が可換環としての準同型写像のとき，f の値域を $f(K)$ に制限した写像を $f'\colon K \to f(K)$ とすると，f' は上の意味で同型写像になる．そこで，K, L が体の場合は，可換環としての準同型写像 $f\colon K \to L$ を**中への同型写像**とか **monomorphism** とか**単射準同型写像**と呼ぶ．

定義 1.4.(多項式環) R を可換環とする．

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0 \quad (n \in \mathbb{N},\, a_0, a_1, \ldots, a_n \in R) \qquad ①$$

を X を変数とする R 係数多項式といい，こういう形の元全体の集合を $R[X]$ と書く．$R[X]$ を (X を変数とする) R 上の **1 変数多項式環** (polynomial ring) という．

$a_n \neq 0$ のとき，n を $\deg f(X)$, $\deg_X f(X)$, $\deg f$ などと書き，f の**次数** (degree) という．ただし，$n = 0$ で $a_0 = 0$ のとき，$f(X)$ を**ゼロ多項式**といい，$\deg 0 = -\infty$ と約束する．他方，$n = 0$ で $a_0 \neq 0$ のときは，$f(X)$ を**定数多項式**といい，$\deg f(X) = 0$ である．また，最高次の係数 a_n が $a_n = 1$ を満たす多項式を**モニック多項式** (monic) という．

帰納的に，$R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n]$ と定義し，$R[X_1, \ldots, X_n]$ を R 上の n **変数多項式環**という．

問題 1.5. R は整域とする．
(1) $f(X)$, $g(X) \in R[X]$ に対し $\deg(f(X)g(X)) = \deg f(X) + \deg g(X)$ であることを証明せよ．
(2) $R[X_1, \ldots, X_n]$ は整域であることを証明せよ．

定義 1.6.(極大イデアル・素イデアル) R は可換環とする．部分集合 $I \subset R$ が「$x, y \in I$, $a \in R$ のとき，$x + y \in I$, $ax \in I$」を満たすとき I は R の**イデアル**であるという．I は R のイデアルで $I \neq R$ とする．「$x, y \in R$, $xy \in I$ ならば $x \in I$ または $y \in I$」が成り立つとき，I は R の**素イデアル**であるという．I は R のイデアルで $I \neq R$ であり，$I \subsetneqq J \subsetneqq R$ を満たすイデアル J が存在しないとき，I は R の**極大イデアル**であるという．

定理 1.7. R は可換環，I はイデアルで $I \neq R$ とする．
(1) I が R の素イデアルであるための必要十分条件は，R/I が整域であることである．
(2) I が R の極大イデアルであるための必要十分条件は，R/I が体であることである．
(3) R の極大イデアルは R の素イデアルである．
(4) R が整域であるための必要十分条件は，(0) が R の素イデアルであることである．

証明. 一般に $a \in R$ に対し，I を法とする a の剰余類を $\overline{a} \in R/I$ と書くことにする．

(1) I は R の素イデアルとする．R/I の 0 でない 2 元 $\overline{a}$, $\overline{b} \in R/I$ $(a, b \in R)$ を取る．$\overline{0}$ でないので $a \notin I$, $b \notin I$ である．I は素イデアルなので $ab \notin I$ である．よって，$\overline{a}\overline{b} \neq \overline{0}$ で，R/I は整域である．

逆に，イデアル $I \subset R$ が素イデアルでなければ，$a \notin I$, $b \notin I$, $ab \in I$ となる $a, b \in R$ が存在する．R/I の 0 でない 2 元 $\overline{a}, \overline{b} \in R/I$ $(a, b \in R)$ このとき，$\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, $\overline{a}\overline{b} = \overline{0}$ となり，R/I は 0 でないゼロ因子を持つので R/I は整域でない．

(2) R/I が体であるとする．自然な全射 $f\colon R \to R/I$ を考える．もし，$I \subsetneqq J \subsetneqq R$ となるイデアル J が存在すれば，$f(J)$ は R/I のイデアルである．R/I のイデアルは (0) と R/I しかない．$f(J) = 0$ ならば $J = I$, $f(J) = R/I$ ならば $J = R$ となり矛盾する．

もし，R/I が体でなければ，0 以外の非可逆元 $\overline{a} \in R/I$ $(a \in R)$ が存在する．$J = I + Ra$ は I のイデアルで，$a \notin I$ だから $I \subsetneqq J$ である．しかし，もし $J = R$ ならば $1 = x + ra$ を満たす $x \in I$, $r \in R$ があり，$\overline{ra} = \overline{1}$ となり，$\overline{a}$ が非可逆元であることに矛盾する．よって，$I \subsetneqq J \subsetneqq R$ で I は極大イデアルでない．

(3) 体は整域であることと，(1), (2) よりわかる．

(4) R は整域とする．$a, b \in R$, $ab \in (0)$ ならば $ab = 0$ であるが，R は整域だから $a = 0$ または $b = 0$ であり，$a \in (0)$ または $b \in (0)$ となる．よって，(0) は素イデアルである．

R が整域でないとすると，$0 \neq a \notin (0)$, $0 \neq b \notin (0)$, $0 = ab \in (0)$ となる $a, b \in R$ があるので，(0) は素イデアルでない． □

定理 1.8. K を体とし，1 変数多項式環 $K[X]$ を考える．以下が成り立つ．

(1) $K[X]$ の (0) 以外のイデアル I は，あるモニック多項式 $f(X) \in K[X]$ により，$I = (f(X))$ と表すことができる．
(2) (0) 以外の素イデアル I は，ある既約なモニック多項式 $p(X)$ により $I = (p(X))$ と書ける．
(3) $0 \neq f(X) \in K[X]$ で $(f(X))$ が素イデアルならば，$f(X)$ は既約多項式である．
(4) I が $K[X]$ の (0) 以外の素イデアルならば，I は極大イデアルである．
(5) $f(X) \in K[X]$ が 1 次以上の既約多項式ならば，$(f(X))$ は $K[X]$ の極大イデアルである．

証明. (1) I を (0) でない $K[X]$ のイデアルとする．I に含まれる次数最小の多項式を $f(X)$ とする．$f(X)$ の最高次の係数を a_n とすると，$a_n^{-1} \in K \subset K[X]$ だから $a_n^{-1} f(X) \in I$ である．よって，はじめから $f(X)$ はモニック多項式であると仮定してよい．

$I = (f(X))$ を示す．勝手な $g(X) \in I$ を取る．$g(X)$ を $f(X)$ で割った商を $q(X)$, あまりを $r(X)$ とする．$\deg r(X) < \deg f(X)$, $r(X) = g(X) - f(X)q(X) \in I$ だから，$\deg f(X)$ の最小性から $r(X) = 0$ で，$g(X) = f(X)g(X) \in (f(X))$ となる．よって，$I = (f(X))$ である．

(2) (1) の結果から，あるモニック多項式により $I = (p(X))$ と書ける．もし，$p(X) = f(X)g(X)$ ($f(X)$, $g(X) \in K[X]$ は 1 次以上の多項式) と因数分解できたとすると，$f(X)$, $g(X)$ は $p(X)$ の倍数でないから I に属さない．よって，I は素イデアルでない．よって $p(X)$ は既約である．

(3) の証明は (2) と同様である．

(4) $I \neq (0)$ は $K[X]$ の素イデアルとする．$I = (p(X))$ と書ける．$I \subset J \subsetneq K[X]$ を満たすイデアル J を取る．$J = (f(X))$ と書ける．$f(X)$ はモニックと仮定してよい．$p(X) \in J$ なので $p(X)$ は $f(X)$ の倍数である．$p(X)$ は既約なモニック多項式なので $p(X) = f(X)$ となり，$I = J$ となる．よって I は極大イデアルである．

(5) $g(X)h(X) \in (f(X))$ ($g(X)$, $h(X) \in K[X]$ は 1 次以上の多項式) とすると，$g(X)h(X)$ は $f(X)$ の倍数で，$f(X)$ は既約だから，$g(X)$ が $h(X)$ は $f(X)$ の倍数である．よって $(f(X))$ は素イデアルである．(4) より，$(f(X))$ は極大イデアルである． □

定義 1.9.(分数体) R は整域とする．このとき，分数の集合

$$Q(R) := \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \neq 0 \right\}$$

は，通常の分数の和，積により体になる．$Q(R)$ を R の**分数体**という．R の元 a と $\frac{a}{1} \in Q(R)$ を同一視して $R \subset Q(R)$ と考える．

分数の意味を正確に書いておく．$X := R \times (R - \{0\})$ とし，$(a, b), (c, d) \in X$ に対し，

$$(a, b) \sim (c, d) \iff ad = bc$$

として X 上に $\sim$ を定義すると，これは X 上の同値関係になる．$Q(R) := X/\sim$ と定義し，(a, b) の同値類を $\frac{a}{b}$ と書く．そして，上で述べたように $Q(R)$ の和と積を，$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ と定義する．このとき，$Q(R)$ が体になることは容易に確認できる．

ただし，R が整域でない可換環の場合は，$\sim$ は X 上の同値関係にならないので，S を R の非零因子全体の集合として，

$$(a, b) \sim (c, d) \iff \text{ある } s \in S \text{ が存在して } (ad - bc)s = 0$$

と変更しないといけない．この話はこの講義で使わないので，詳細は省略する．

問 1.10. 上の定義において，$\sim$ が X 上の同値関係であることと，$Q(R)$ が体であることを証明せよ．

定義 1.11.(有理関数体) K は体とし，$K[X_1, \ldots, X_n]$ は n 変数多項式環とする．その分数体 $Q(K[X_1, \ldots, X_n])$ を $K(X_1, \ldots, X_n)$ と書き，K 上の n 変数**有理関数体**という．$K(X_1, \ldots, X_n)$ の元 $f(X_1, \ldots,$

$X_n)/g(X_1,\ldots, X_n)$ (ただし，$f(X_1,\ldots, X_n), g(X_1,\ldots, X_n) \in K[X_1,\ldots, X_n]$) を K 上の**有理関数**とか**有理式**という．

2．代数拡大

体の代数拡大と整域の整拡大の話は，途中までほとんど並行しているので，後の便を考えて，しばらく整拡大の用語も含めて説明する．

定義 2.1.(拡大体・部分体) R, S が可換環で $R \subset S$ であり，R 上の和と積は S 上の和と積を R の元に適用したものと一致していて，かつ R の単位元 1_R と S の単位元 1_S が一致するとき，R は S の**部分環**，S は R の**拡大環**であるという．S が整域の場合は R は S の**部分整域**，S は R の**拡大整域**であるという．

K と L が体で K が L の部分環のとき，K は L の**部分体**, L は K の**拡大体**であるという．このとき，L は K-ベクトル空間になっている．また $K \subset M \subset L$ を満たす体 M を K と L の**中間体**という．

R は可換環で S は R の拡大環とする．また，$c_1,\ldots, c_n \in S$ とする．R と $c_1,\ldots, c_n$ を含む S の最小の部分環を $R[c_1,\ldots, c_n]$ と書き，R 上 $c_1,\ldots, c_n$ で**生成される環**という．$R[c_1,\ldots, c_n]$ という記号は多項式環 $R[X_1,\ldots, X_n]$ とまぎらわしい記号であるが，文脈で判断するしかない．なお，$f(X_1,\ldots, X_n) \in R[X_1,\ldots, X_n]$ に対し，各 X_i に c_i を代入したとき $f(c_1,\ldots, c_n) \in R[c_1,\ldots, c_n]$ となる．$f(X_1,\ldots, X_n) \in R[X_1,\ldots, X_n]$ に対して $f(c_1,\ldots, c_n) \in R[c_1,\ldots, c_n]$ を対応させる写像を $\varphi : R[X_1,\ldots, X_n] \longrightarrow R[c_1,\ldots, c_n]$ とすると，φ は環としての準同型写像で全射であり，準同型定理から，

$$R[c_1, \ldots, c_n] \cong R[X_1, \ldots, X_n]/\operatorname{Ker}\varphi$$

が成り立つ

K は体で L は K の拡大環とする．$c_1,\ldots, c_n \in L$ とする．K と $c_1,\ldots, c_n$ を含む K の最小の部分体を $K(c_1,\ldots, c_n)$ と書き，K 上 $c_1,\ldots, c_n$ で**生成される体**という．こちらについては，有理関数体からの準同型写像 $\varphi : K(X_1,\ldots, X_n) \longrightarrow K(c_1,\ldots, c_n)$ は一般には**存在しない**ので注意すること．つまり，X_i に c_i に代入したときに分母が 0 になることがあって，そういう写像が定義できない．しかし，

$$K(c_1, \ldots, c_n) = Q\big(K[c_1, \ldots, c_n]\big)$$

は成立する．

定義 2.2.(整拡大・代数拡大) R は整域，$K = Q(R)$ は R の分数体, L は K を含む体とする．$z \in L$ に対し，ある自然数 n と $a_0, a_1,\ldots, a_{n-1} \in R$ が存在して

$$z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_2z^2 + a_1z + a_0 = 0 \qquad ①$$

を満たすとき，z は R 上**整** (integral) であると言う．$z \in R$ ならば z は R 上整である ($n = 1, a_0 = -z \in R$ とすればよい)．特に，R が体のとき，R 上整な元を R 上**代数的** (algebraic) と言い，R 上代数的でない元を R 上**超越的** (transcendental) と言う．

R 上整な元 z に対し，① を満たす R 上のモニック多項式のうち，2 つの 1 次以上の R 上のモニック多項式の積に表せない多項式を x の R 上の**最小多項式**と呼ぶ．例えば，R が UFD であれば z の最小多項式は一意的に定まるが，一般の整域 R では z の最小多項式は必ずしも一意的でないことに注意する．特に，R が体の場合には z の最小多項式は一意的である．

R を含む整域 S の各元が R 上整であるとき，S は R 上**整**であるとか，S は R の**整拡大** (integral extension) である言う．特に，R, S が体で，S が R 上整のとき，S は R 上**代数的**であるとか，S は R の**代数拡大**であると言う．S が R 上代数的でないとき，S は R 上**超越的**であるとか，S は R の**超越拡大**であると言う．

$x_1,\ldots, x_n \in S$ に対し，R-多元環として $R[X_1,\ldots, X_n] \cong R[x_1,\ldots, x_n]$ (左辺は多項式環) であるとき，$x_1,\ldots, x_n$ は R 上**代数的独立**であると言い，代数的独立でないとき**代数的従属**であると言う．

問 2.3. 上の定義において，R が UFD のとき R 上整な元 $z \in S$ の R 上の最小多項式は一意的であることを証明せよ．R が UDF ならば $R[X]$ も UFD であることは認めて用いてよい．

定理 2.4. 定義 2.2 と同じ記号を用いる．$z \in L$ とする．
(1) $M \neq 0$ が $R[z]$-加群で，R-加群として有限生成ならば，z は R 上整である．

(2) z が R 上整であるための必要十分条件は，$R[z]$ が有限生成 R-加群であることである．

証明. (1) $M = Rx_1 + \cdots + Rx_n$ とする．M は $R[z]$-加群だから，$zx_i \in M$ であり．

$$zx_i = \sum_{j=1}^{n} a_{ij}x_j \quad (a_{ij} \in R)$$

と書ける．a_{ij} を (i, j)-成分とする n 次正方行列を A, n 次の単位行列を I, $f(z) = \det(zI - A)$ とおくと，体 $Q(R[z])$ の元を成分とする行列とベクトルとして，連立方程式 $(zI - A)\mathbf{x} = \mathbf{0}$ がゼロベクトル以外の解を持つから，$f(z) = 0$ である．$f(z)$ は z^n の係数が 1 の，z についての n 次式だから，z は R 上整である．

(2) z が R 上整ならば ① を満たすから，逆に，$R[z]$ が有限生成 R-加群ならば，(1) を $M = R[z]$ として用い入れば z は R 上整となる． □

定理 2.5. 定義 2.2 と同じ記号を用いる．
(1) $z \in L$ が R 上整で，$w \in L$ が $R[z]$ 上整ならば，w は R 上整である．
(2) $x, y \in L$ が R 上整ならば，$x + y$ と xy も R 上整である．
(3) R が体で，$0 \neq x \in L$ が R 上代数的ならば，$1/x$ は R 上代数的である．
(4) S が R の整拡大ならば，$Q(S)$ は $Q(R)$ の代数拡大である．
(5) 整域 S が体 R 上整ならば S は体である．

証明. (1) $w \in L$ が $R[z]$ 上整ならば，$(R[z])[w] = R[z, w]$ も有限生成 R-加群だから，w は R 上整である．

(2) $R[x, y]$ は有限生成 R-加群だから，$x + y$, xy は R 上整である．

(3) x が R 上代数的ならば，$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ $(a_i \in R)$ と書ける．$a_0 \neq 0$ と仮定してよい．すると，

$$\frac{1}{x^n} + \frac{a_1}{a_0} \cdot \frac{1}{x^{n-1}} + \cdots + \frac{a_{n-1}}{a_0} \cdot \frac{1}{x} + \frac{1}{a_0} = 0$$

なので，$1/x$ は R 上代数的である．

(4) は明らかである．

(5) $x \in S$ が (3) の証明のように表せるとき，

$$\frac{1}{x} = -\frac{1}{a_0}(x^{n-1} + a_{n-1}x^{n-1} + \cdots + a_2x + a_1) \in S$$

なので，S は体である． □

定理&定義 2.6. (1) K は体で L は K の拡大体とする．このとき，L は K-ベクトル空間とみなせるが，L が有限次元 K-ベクトルならば，L は K の代数拡大である．このとき，L は K の**有限 (次) 代数拡大**であるといい，その次元を $[L : K] = \dim_K L$ と書き，L の K 上の**拡大次数**という．

(2) K は体で L は K の有限次代数拡大体, M は L の有限次代数拡大体とする．すると，M は K の有限次代数拡大体で，

$$[M : K] = [M : L] \cdot [L : K]$$

が成り立つ．

証明. (1) 定理 2.4 からすぐわかる．

(2) $l = [L : K]$ とし $x_1, \ldots, x_l \in L$ を K-ベクトル空間 L の基底とする．また，$m = [M : L]$ とし $y_1, \ldots, y_m \in M$ を L-ベクトル空間 M の基底とする．lm 個の元の集合 $B := \{x_iy_j \mid 1 \leqq i \leqq l, 1 \leqq j \leqq m\}$ が K-ベクトル空間 M の基底であることを示せばよい．

B が K 上 1 次独立であることを示す．$\displaystyle\sum_{i=1}^{l}\sum_{j=1}^{m} a_{ij}x_iy_j = 0$ $(a_{ij} \in K)$ とする．$b_j := \displaystyle\sum_{i=1}^{l} a_{ij}x_i \in L$ とおく．$\displaystyle\sum_{j=1}^{m} b_jy_j = \sum_{i=1}^{l}\sum_{j=1}^{m} a_{ij}x_iy_j = 0$ で，$y_1, \ldots, y_m$ は L 上 1 次独立なので，$b_1 = \cdots = b_m = 0$ である．

$\sum_{i=1}^{l} a_{ij}x_i = b_j = 0$ で，$x_1,\ldots, x_l$ は K 上 1 次独立なので，$a_{1j} = \cdots = a_{lj} = 0$ である．

B が K 上 M を生成することを示す．勝手な $z \in M$ を取る．ある $b_1,\ldots, b_m \in L$ により，$z = \sum_{j=1}^{m} b_j y_j$ と書ける．また，ある $a_{1j},\ldots, a_{lj} \in K$ により，$b_j = \sum_{i=1}^{l} a_{ij}x_i$ と書ける．すると，$z = \sum_{i=1}^{l}\sum_{j=1}^{m} a_{ij}x_i y_j$ なので，B は K 上の M の基底である． □

定理&定義 2.7. K は体で L は K の拡大体とする．$z \in L$ は K 上代数的とし，その K 上の最小多項式を $f_z(X)$ とする．このとき，$K[z]$ は体で，$[K[z] : K] = \deg f_z(X)$ が成り立つ．したがって，$K(z) = K[z]$ である．$d := [K(z) : K]$ とおくとき，z は K 上 d **次**の代数的元であるとか，z の K 上の**次数**は d であるという．

証明. $K[z] \subset L$ は整域で K 上整だから，定理 2.5(5) より $K[z]$ は体である．$K(z) = Q(K[z])$ で $K[z]$ が体だから $K(z) = K[z]$ である．

$f(X) \in K[X]$ に $f(z) \in K[z]$ を対応させる準同型写像を $\varphi\colon K[X] \longrightarrow K[z]$ とするとき，$\mathrm{Ker}\,\varphi = (f_z(X))$ ($f_z(X)$ で生成される $K[X]$ の単項イデアル) であるから，準同型定理により

$$K[x] \cong K[X]/(f_z(X))$$

である．$\deg f_z(X) = d$, $f_z(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$ ($c_0,\ldots, c_{d-1} \in K$) とするとき，$K[z]$ は K 上 $1, z, z^2,\ldots, z^{d-1}$ で生成される．($z^d = -c_{d-1}z^{d-1} - \cdots - c_1z - c_0$ に注意せよ.) $1, z, z^2,\ldots, z^{d-1}$ が K 上 1 次従属だとすると，その関係式が与える多項式は，最小多項式の次数より小さくなり矛盾する．よって，$1, z, z^2,\ldots, z^{d-1}$ は $K[z]$ の K 上の基底である． □

3. 体の標数と正標数の体の基本性質

第 1 回に説明したように，体 K において，$\underbrace{1+1+\cdots+1}_{p\text{ 個}} = 0$ となる最小の自然数 p を K の**標数**いった．ただし，何個 1 を足しても 0 にならないとき，K の標数は 0 である．体 K の標数を $\mathrm{char}\,K$ と表す.

定理 3.1. 体 K の標数は 0 か素数である.

証明. 今，体 K の標数 p は 0 でないと仮定する．$0 \neq 1 \in K$ だから，$p \geqq 2$ である．一般に任意の加群は $\mathbb{Z}$-加群と考えられるから，K も $\mathbb{Z}$-加群とみなせる．K の単位元 $1 = 1_K$ に $n \in \mathbb{Z}$ を作用させて得られる K の元を $\overline{n} = n \cdot 1_K \in K$ と書くことにする．

さて，$p = km$ (k, m は 2 以上の整数) であったとすると，すると，$\overline{k}\,\overline{m} = \overline{mn} = \overline{p} = 0$ となる．$\overline{k} \neq 0$, $\overline{m} \neq 0$ だから，これは K が体であることに矛盾する． □

定義 3.2.(素体) p が素数のとき $p\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルなので $\mathbb{Z}/p\mathbb{Z}$ は体である．$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ と書き，これを**標数** p **の素体**という．また，$\mathbb{Q}$ を標数 0 の素体という．素体は体に含まれる最小の部分体で，$\mathbb{F}_p$ (p は素数) と $\mathbb{Q}$ だけである．なお，有限個の元からなる体を**有限体**, 無限個の元からなる体を**無限体**という.

定理 3.3. K は体で $p := \mathrm{char}\,K \neq 0$ とする．また，$e \in \mathbb{N}$, $q = p^e$ とおく (p^e を**準素数**ともいう)．このとき，任意の $a_1,\ldots, a_n \in K$ に対し，

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q$$

が成り立つ.

証明. (1) $e=1$, $n=2$ の場合を考える．$a=a_1$, $b=a_2$ とする．$1 \leqq k < p$ のとき二項係数

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!} \in \mathbb{N} \qquad ①$$

を考える．$k<p$ なので ① の分母 k は p で割り切れない．しかし，① の分母は p の倍数なので，$\binom{p}{k}$ は p の倍数である．$(a+b) = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k}$ であるが，$\binom{p}{k} \cdot 1_K = 0 \in K$ なので，$(a+b)^p = a^p + b^p$ である．

(2) 今，$(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$ が任意の a_1,..., $a_n \in K$ に対して成立すると仮定する．勝手な $a_{n+1} \in K$ を取る．(1) と帰納法の仮定から，

$$a_1^p + \cdots + a_{n+1}^p = (a_1 + \cdots + a_n)^p + a_{n+1}^p = (a_1 + \cdots + a_n + a_{n+1})^p$$

が成り立つ．

(3) $q=p^e$, $r=p^{e+1}$ とおく．$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q$ が任意の a_1,..., $a_n \in K$ に対して成立すると仮定する．$(a_i^q)^p = a_i^r$ なので，

$$(a_1 + \cdots + a_n)^r = \big((a_1 + \cdots + a_n)^q\big)^p = (a_1^q + \cdots + a_n^q)^p = a_1^r + \cdots + a_n^r$$

となる． □

定理 3.4. K が n 個の元からなる有限体ならば，ある素数 p とある $e \in \mathbb{N}$ により $n = p^e$ と書ける．また，任意の $a \in K$ に対して，

$$a^n = a$$

が成り立つ．

証明. $p := \operatorname{char} K \neq 0$ だから，p は素数である．$K \supset \mathbb{F}_p$ で，K は $\mathbb{F}_p$-ベクトル空間であるから，$e := \dim_{\mathbb{F}_p} K$ とおけば $n = p^e$ である．

$K^\times := K - \{0\}$ とおく．$K^\times$ は乗法 $\times$ について位数 $(n-1)$ のアーベル群である．よって，任意の $a \in K^\times$ に対して $a^{n-1} = 1$ である．これより $a^n = a$ となる．$a=0$ のときも $a^n = 0 = a$ である． □

実は，K が有限体ならば，乗法群 $K^\times := K - \{0\}$ は巡回群になるのであるが，その証明の準備としてオイラーのファイ関数の説明をする．

定義 3.5. 自然数 n に対し，1, 2, 3..., $n-1$ の中で　n と互いに素な整数の個数を $\varphi(n)$ で表し，$\varphi(n)$ を**オイラーのファイ関数**という．一般に $k \in \mathbb{Z}$ に対し，その $n\mathbb{Z}$ を法とする同値類を $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ とするとき，$\overline{k}$ が $\mathbb{Z}/n\mathbb{Z}$ で可逆であることと，$\mathrm{GCD}(k, n) = 0$ は同値であるから，$\mathbb{Z}/n\mathbb{Z}$ の中の可逆元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^\times$ と書くことにするとき，乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数が $\varphi(n)$ である．

定理 3.6. 自然数 n を $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ (p_1,..., p_r は相異なる素数) と素因数分解する．すると，

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

である．

証明. n 未満の n と互いに素な自然数全体の集合を A とする．定義から $\varphi(n) = \#A$ である．($\#A$ は集合 A の要素の個数を表す.) 集合 B を

$$B := \left\{ (b_1, b_2, \ldots, b_r) \;\middle|\; \begin{array}{l} \text{各 } i = 1,\ldots, r \text{ に対し，} b_i \text{ は} \\ p_i \text{ と互いに素な } p_i^{e_i} \text{ 未満の自然数} \end{array} \right\}$$

とおく．$k \in A$ に対し，k を $p_i^{e_i}$ で割った余りを k_i $(i = 1,\ldots, r)$ とし，$f(k) = (k_1, k_2,\ldots, k_r)$ とする．$f(k) \in B$ である．

逆に，$(b_1, b_2,\ldots, b_r) \in B$ を任意に選んだとき，中国剰余定理より，k を $p_i^{e_i}$ で割った余りが b_i $(i = 1,\ldots, r)$ となるような n 未満の自然数 $k \in A$ が存在する．よって，写像 $f\colon A \to B$ は全単射であり，$\#A = \#B$ となる．

ところで，p_i と互いに素な $p_i^{e_i}$ 未満の自然数の個数は $p_i^{e_i-1}(p_i-1)$ である．よって，$\#B = \prod_{i=1}^{r} p_i^{e_i-1}(p_i-1)$ である． □

定理 3.7. 自然数 n の正の約数全体の集合を $D(n)$ とするとき，

$$\sum_{d\in D(n)} \varphi(d) = n$$

が成り立つ．

ここで $\sum_{d\in D(n)} \varphi(d)$ は $D(n)$ のすべての元 d について $\varphi(d)$ の和をとることを表す．

証明. $X(n) = \{1, 2,\ldots, n\}$ とし，$d \in D(n)$ に対し，

$$A_d = \{x \in X(n) \mid \mathrm{GCD}(n, x) = n/d\}, \quad B_d = \{x \in X(d) \mid \mathrm{GCD}(d, x) = 1\}$$

とおく．写像 $f\colon B_d \longrightarrow A_d$ を $f(x) = nx/d$ で定めれば，f は全単射である．よって，$\#A_d = \#B = \varphi(d)$ である．また，$\bigcup_{d\in D(n)} A_d = X(n)$ だから，$\sum_{d\in D(n)} \varphi(d) = n$ がわかる． □

補題 3.8. $n \in \mathbb{N}$, K は体として，$G := \{x \in K \mid x^n = 1\}$ とする．すると，G は積 (乗法) について巡回群になる．

証明. $x \in K^\times$ に対し $x^m = 1$ を満たす最小の自然数 m を $m = \mathrm{ord}(x)$ と書くことにする．$\#K = p^e$, $n := p^e - 1$ とおく．

(1) n の約数 $d \in D(n)$ に対し $\mathrm{ord}(x) = d$ を満たす $x \in G$ は丁度 $\varphi(d)$ 個存在することを示す．

$d \in D(n)$ に対し，

$$X_d = \{x \in G \mid x^d = 1\}, \quad Y_d = \{x \in G \mid \mathrm{ord}(x) = d\}$$

とおく．K は体だから d 次方程式 $x^d = 1$ の解 x は高々 d 個しか存在せず，$\#X_d \leqq d$ である．

もし，$Y_d \neq \phi$ ならば，$a \in Y_d$ を取ると，$X_d = \{1, a, a^2,\ldots, a^{d-1}\}$ であり，$\#X_d = d$ となる．また，$Y_d = \{a^i \mid \mathrm{GCD}(i, d) = 1,\ 1 \leqq i < d\}$ であるので，$\#Y_d = \varphi(d)$ である．

$Y_d = \phi$ ならば，$\#Y_d = 0$ である．$X_n = G$, $X_{p-1} = \bigcup_{d\in D(p-1)} Y_d$ より，

$$n = \#X_n = \bigcup_{d\in D(n)} \#Y_d \leqq \sum_{d\in D(n)} \varphi(d) = n$$

となり，$\leqq$ は $=$ で，任意の $d \in D(n)$ に対し，$\#Y_d = \varphi(d)$ が成り立つ．

(2) $\varphi(n) \neq 0$ なので，$\mathrm{ord}(x) = n$ を満たす $x \in G$ が存在する．すると，G は x で生成される巡回群である． □

定理 3.9. K が有限体ならば，乗法群 $K^\times := K - \{0\}$ は巡回群である．

証明. $\#K = p^e$, $n := p^e - 1$ とおく．$G := K^\times$ とおくと，$G = \{x \in K \mid x^n = 1\}$ であるので，前補題より，$G = K^\times$ は巡回群である． □

4. 分解体

定義 4.1. K, L は体，$\sigma\colon K \to L$ は中への同型写像．$f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in K[K]$ とする．このとき，

$$\sigma(f(X)) = \sigma(c_n)X^n + \sigma(c_{n-1})X^{n-1} + \cdots + \sigma(c_1)X + \sigma(c_0) \in L[X]$$

と書くことにする．ただし，変数 X に σ を作用させないこをを強調する場合には，$\sigma(f(X))$ ではなく $\sigma(f)(X)$ と書く場合もある．これは，X に K に属さない元を X に代入するときに問題になるが，通

常，代入する元が σ の定義域に属さない元の場合，それには σ を作用させない．変数 X を省略して $f \in K[X]$ に対し，$\sigma(f) \in L[X]$ などのような書き方もする．$\sigma(f(X))$ を $f^{\sigma}(X)$ と表わしている文献も多い．

また，$\tau\colon L \to M$ が体 M への中への同型写像のとき，$(\tau \circ \sigma)(f(X))$ を $\tau\sigma(f(X))$ とか，$f^{(\tau\sigma)}(X)$ とか $f^{\sigma\tau}(X)$ と書く．写像を f の右上に付けた場合の合成写像の順序に注意する．この講義ノートではその書き方は使わない．

定義 4.2. K は体，L は K の拡大体, $f(X) \in K[X]$ は 1 次以上の多項式とする．自然に $K[X] \subset L[X]$ と考えたとき，$L[X]$ において，$f(X) = a(X - c_1)(X - c_2)\cdots(X - c_n)$ $(a \in K;\, c_1,\ldots,\, c_n \in L)$ と 1 次式の積に因数分解できるとき，L は $f(X)$ の**分解体**であるという．

L が $f(X)$ の分解体で，M は K と L の中間体 $(K \subset M \subsetneqq L)$ で，M が $f(X)$ の分解体になっているようなものが存在しないとき，L は $f(X)$ の**最小分解体**であるという．

定理 4.3. K は体，$f(X) \in K[X]$ は 1 次以上の多項式とする．

(1) $f(X)$ が $K[X]$ で既約ならば，$L = K[X]/(f(X))$ は K の有限次代数拡大体で，$X \in K[X]$ のイデアル $(f(X))$ を法とする同値類を $\alpha \in L$ とすると，$f(\alpha) = 0$ が成り立つ．

(2) $f(X)$ の最小分解体は存在する．

(3) L_1, L_2 が $f(X)$ の最小分解体ならば，同型写像 $\sigma\colon L_1 \to L_2$ で $\sigma|_K = \mathrm{id}_K$ (K 上の恒等写像) を満たすものが存在する．

証明. (1) $f(X) \in K[X]$ が既約ならば，$(f(X))$ は $K[X]$ の極大イデアルなので $K[X]/(f(X))$ は体になる．$\dim_K K[X]/(f(X)) = \deg f(X) < \infty$ だから，$K[X]/(f(X))$ は K の有限次代数拡大体である．$f(\alpha)$ は $f(X)$ のイデアル $(f(X))$ を法とする同値類だから，$f(\alpha) = 0$ である．

(2) $f(X)$ の次数に関する帰納法で証明する．ただし，体 K は途中で変わる．

$\deg f(X) = 1$ ならば，K 自身が K の最小分解体である．

$\deg f(X) \geqq 2$ とする．

(2) $f(X)$ を $K[X]$ で因数分解し，$f(X)$ の約数であるような既約な多項式 $p(X) \in K[X]$ を 1 つ取る．$L := K[X]/(p(X))$ とおくと，(1) より $p(\alpha) = 0$ を満たす $\alpha \in L$ が存在する．$f(\alpha) = 0$ でもあるので，$L[X]$ において $f(X) = (X - \alpha)g(X)$ $(\exists g(X) \in L[X])$ と因数分解できる．$g(X) \in L[X]$ と考えて，体を L に取り替えて帰納法の仮定を使うと，$\deg g(X) < \deg f(X)$ だから，L を含む $g(X)$ の最小分解体 M が存在する．$g(X) = a(X - c_1)(X - c_2)\cdots(X - c_n)$ $(a \in L;\, c_1,\ldots,\, c_n \in M)$ と 1 次式の積に因数分解できる．ここで a は $f(X)$ の最高次の項と等しいので，$a \in K$ である．M 内で K と α と $c_1,\ldots,\, c_n$ を含む最小の体を F とすれば，それが $f(X)$ の最小分解体である．

(3) $f(X)$ の次数に関する帰納法を使うために，命題を少し一般化した次の命題 (P_n) を証明する．(P_n) を $K_1 = K_2 = K$, $\tau = \mathrm{id}_K$ として用いればよい．

(P_n) K_1, K_2 は体で同型写像 $\tau\colon K_1 \to K_2$ が存在すると仮定する．$f(X) \in K[X]$ で $1 \leqq \deg f(X) \leqq n$ とする．L_1 は $f(X)$ の最小分解体，L_2 は $\tau(f(X))$ の最小分解体とする．すると，同型写像 $\sigma\colon L_1 \to L_2$ で $\sigma|_{K_1} = \tau$ を満たすものが存在する．

$\deg f(X) = 1$ ならば $L_1 = K_1$, $L_2 = K_2$ だから (P_1) は自明である．

$n \geqq 2$ とし (P_{n-1}) を仮定する．(1) の証明のように，$f(X)$ の因子 $p(X) \in K_1[X]$ を 1 つ取る．$\deg p(X) = 1$ ならば $f(X) = (X - \alpha)g(X)$ $(\alpha \in K_1,\, g(X) \in K[X])$ と書け，L_1 は $g(X)$ の最小分解体，L_2 は $\tau(g(X))$ の最小分解体だから，$g(X)$ に (P_{n-1}) を適用すると，同型写像 $\sigma\colon L_1 \to L_2$ の存在がわかる．

$\deg p(X) \geqq 2$ の場合を考える．$p(X)$ の L_1 における根の 1 つを $\alpha \in L_1$ とし，$\sigma(p(X))$ の L_2 における根の 1 つを $\beta \in L_1$ とする．$K_1(\alpha) \cong K_1[X]/(p(X)) \cong K_2[X]/(\sigma(p(X))) \cong K_2(\beta)$ なので，$\tau'(\alpha) = \beta$ を満たす同型写像 $\tau'\colon K_1(\alpha) \longrightarrow K_2(\beta)$ が存在して，$\tau'|_{K_1} = \tau$ を満たす．$f(X) = (X - \alpha)g(X)$ を満たす $g(X) \in K_1(\alpha)[X]$ が存在する．$\tau(f(X)) = \tau'(f(X)) = (X - \tau'(\alpha))\tau'(g(X)) = (X - \beta)\tau'(g(X))$ である．L_1 は $g(X)$ の最小分解体，L_2 は $\tau'(g(X))$ の最小分解体である．帰納法の仮定 (P_{n-1}) から，同型写像 $\sigma\colon L_1 \to L_2$ で $\sigma|_{K_1(\alpha)} = \tau'$ を満たすものが存在する．$\tau'|_{K_1} = \tau$ より $\sigma|_{K_1} = \tau$ である． □

L が $f(X) \in K[X]$ の最小分解体で $\deg f(X) = n$ のとき，$[L : K] \leqq n!$ であることが，上の (2) の証明からわかる．このことについては，後の章で詳しく考察する．

定義 4.4.(共役) K は体，L は K の拡大体，$a, b \in L$ とする．ある既約多項式 $f(X) \in K[X]$ が存在して，$f(a) = f(b) = 0$ を満たすとき，a と b は K 上**共役** (conjugate) であるという．

$$\mathrm{Aut}(L/K) := \left\{\sigma\colon L \to L \;\middle|\; \sigma \text{ は体としての同型写像で，} \sigma|_K = \mathrm{id}_K\right\}$$

を K 上の L の**自己同型群**という．ここで $\mathrm{id}_K\colon K \to K$ は K 上の恒等写像を表す．なお，$\mathrm{Aut}(L/K)$ は写像の合成を演算として群になる．また，1, 2,..., n の置換全体の群 (n **次対称群**) を，$\mathfrak{S}_n$ という記号で表す．

$K \subset M_1 \subset L$, $K \subset M_2 \subset L$ を満たす体 M_1, M_2 に対し，ある同型写像 $\sigma\colon M_1 \to M_2$ で，$\sigma|_K = \mathrm{id}_K$ を満たすものが存在するとき，M_1 と M_2 は K 上**共役**であるという．

定理 4.5. K は体，$f(X) \in K[X]$ は既約多項式で，L は $f(X)$ の最小分解体とする．$f(X)$ の L における相異なる根全体を α_1,..., α_n とする．勝手な $\sigma \in \mathrm{Aut}(L/K)$ を取る．すると，$\sigma(\alpha_1)$,..., $\sigma(\alpha_n)$ は $f(X)$ の L における相異なる根全体である．つまり，σ は α_1,..., α_n の置換を引き起こす．この置換を添え字の 1,..., n の置換と考えたものを $\varphi(\sigma) \in \mathfrak{S}_n$ とする．これにより $\varphi\colon \mathrm{Aut}(L/K) \longrightarrow \mathfrak{S}_n$ を定めると，φ は群としての単射準同型写像になる．この φ を通して $\mathrm{Aut}(L/K) \subset \mathfrak{S}_n$ と考える．

証明. σ は $f(X)$ の係数には恒等写像として作用するから，$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ である．また，σ は全単射だから $\alpha_i \neq \alpha_j$ ならば $\sigma(\alpha_i) \neq \sigma(\alpha_j)$ である．よって，$\sigma(\alpha_1)$,..., $\sigma(\alpha_n)$ は $f(X)$ の L における相異なる根全体である．

$\varphi(\tau \circ \sigma) = \varphi(\tau) \circ \varphi(\sigma)$, $\varphi(\sigma^{-1}) = \varphi(\sigma)^{-1}$ は容易にわかるので，φ は準同型写像である．

φ が単射であることを示す．φ は準同系写像だから，$\sigma(\alpha_i) = \alpha_i$ ($1 \leqq \forall i \leqq n$) ならば $\sigma = \mathrm{id}_L$ であることを示せばよい．L は $f(X)$ の K 上の最小分解体だから，$L = K(\alpha_1,..., \alpha_n)$ である．つまり $\mathrm{Aut}(L/K)$ の元は α_1,..., α_n の行き先だけで決定される．よって，結論を得る． □

5. 代数閉包

今回の内容は証明が少し難しいが，先に済ませておいたほうが後の議論が楽になる．

定理&定義 5.1. K を体とするとき，以下の 4 条件は同値である．K がそのいずれか (したがって，すべて) を満たすとき，K は**代数 (的) 閉体**であるという．
(1) K の代数拡大体は K 以外に存在しない．
(2) $K[X]$ の既約多項式は 1 次である．
(3) $K[X]$ の任意の 1 次以上の多項式は，$K[X]$ の中で 1 次式の積に因数分解できる．
(4) $K[X]$ の 1 次以上の多項式は，K 内に少なくとも 1 つ根を持つ．

証明. (1) $\Longrightarrow$ (2) を示す．$f(X) \in K[X]$ は既約多項式とする．もし $\deg f(X) \geqq 2$ ならば，$f(X)$ の K 上の最小分解体 L は，$K \subsetneqq L$ を満たす K の代数拡大体になり，(1) と矛盾する．

(2) $\Longrightarrow$ (3) と (4) $\Longrightarrow$ (4) は自明である．

(4) $\Longrightarrow$ (1) を示す．L を K の代数拡大体で $L \supsetneqq K$ であるとする．$a \in L - K$ を取り，a の K 上の最小多項式を $f_a(X) \in K[X]$ とする．$f_a(X)$ は $K[X]$ で既約であるが，もし $\deg f_a(X) \geqq 2$ ならば，$f_a(X)$ は K 内に根を満たない．よって $\deg f_a(X) = 1$ であり，$a \in L$ となって矛盾する． □

定義 5.2. K は体とする．L が K の代数拡大体であって，L が代数閉体であるとき，L は L の**代数 (的) 閉包**であるという．

定理 5.3. K は体とする．
(1) K の代数閉包 L は存在する．
(2) L_1, L_2 が K の代数閉包ならば，同型写像 $\sigma\colon L_1 \to L_2$ で $\sigma|_K = \mathrm{id}_K$ を満たすものが存在する．

証明. (1) $K[X]$ 内のすべての既約モニック多項式の集合を $P = \left\{f_\lambda(X) \;\middle|\; \lambda \in \Lambda\right\}$ とする．$f_\lambda \in P$ ($\lambda \in \Lambda$) に対し，$n_\lambda := \deg f_\lambda(X) \in \mathbb{N}$ とおく．また n_λ 個の変数 (K 上代数的独立な不定元) $X_1^{(\lambda)}$,

$X_2^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}$ を取り，K 上の $(1+n_\lambda)$ 変数多項式環 $F_\lambda := K[X, X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}]$ を作る．

$$g_\lambda\big(X, X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}\big) := f_\lambda(X) - \prod_{i=1}^{n_\lambda}\big(X - X_i^{(\lambda)}\big) \in F_\lambda$$

とおく．この多項式を X について整理して X^k の係数を

$$a_k^{(\lambda)} = a_k^{(\lambda)}\big(X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}\big) \in K[X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}]$$

とおく．

$$g_\lambda\big(X, X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}\big) = \sum_{k=0}^{n_\lambda} a_k^{(\lambda)}\big(X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}\big)\cdot X^k = \sum_{k=0}^{n_\lambda} a_k^{(\lambda)} X^k$$

である．

すべての $\lambda\in\Lambda$ についての $X_1^{(\lambda)},\ldots, X_{n_\lambda}^{(\lambda)}$ の集合を $\mathfrak{X} := \big\{X_i^{(\lambda)} \bigm| \lambda\in\Lambda,\ 1\leqq i\leqq n_\lambda\big\}$ とし，すべての $\mathfrak{X}$ の元を変数とする K 上の多項式環を $K[\mathfrak{X}]$ と書くことにする．$K[\mathfrak{X}]$ の元 h は，有限個の $Y_1,\ldots, Y_m\in\mathfrak{X}$ を適当に選べば $h\in K[Y_1,\ldots, Y_m]$ と考えられる．また，任意の $\lambda\in\Lambda$ に対して $F_\lambda\subset K[\mathfrak{X}]$ とみなせる．

$K[\mathfrak{X}]$ の中で $A := \big\{a_k^\lambda \bigm| \lambda\in\Lambda,\ 1\leqq i\leqq n_\lambda\big\}$ を含む最小のイデアルを I とする．

(i) $I\neq K[\mathfrak{X}]$ を証明する．

もし $I = K[\mathfrak{X}]$ ならば，$1\in I$ であるから，ある有限個の $a_{k_1}^{(\lambda_1)},\ldots, a_{k_m}^{(\lambda_m)}\in A$ と，$b_{\lambda_1},\ldots, b_{\lambda_m}\in K[\mathfrak{X}]$ をうまく選んで，$\displaystyle\sum_{i=1}^{m} a_{k_i}^{(\lambda_i)} b_{\lambda_i} = 1$ となるようにできる．ここで，$b_{\lambda_i}\neq 0$ と仮定してよい．$f_{\lambda_1}(X)\cdots f_{\lambda_m}(X)\in K[X]$ の最小分解体を F とする．ある $\alpha_{i,j}\in F$ $(1\leqq i\leqq n,\ 1\leqq j\leqq n_{\lambda_i})$ を選んで，

$$f_{\lambda_i}(X) = \prod_{j=1}^{n_{\lambda_i}}(X-\alpha_{i,j}) \in F[X]$$

となるようにできる．このとき，$g_{\lambda_i}\big(X, \alpha_{i,1},\ldots, \alpha_{i,n_{\lambda_i}}\big) = 0$ となる．よって，$a_{k_i}^{(\lambda_i)}\big(\alpha_{i,1},\ldots, \alpha_{i,n_\lambda}\big) = 0$ である．これは，$\displaystyle\sum_{i=1}^{m} a_{k_i}^{(\lambda_i)} b_{\lambda_i} = 1$ と矛盾する．

(ii) そこで，I を含む $K[\mathfrak{X}]$ の極大イデアル $\mathfrak{m}$ を取り，$L := K[\mathfrak{X}]/\mathfrak{m}$ とおく．L は K の拡大体である．$X_i^{(\lambda)}\in\mathfrak{X}$ に対し，その $\mathfrak{m}$ を法とする同値類を $\beta_i^{(\lambda)}\in L$ とする．$A\subset\mathfrak{m}$ だから $a_k^\lambda\big(\beta_1^{(\lambda)},\ldots, \beta_{n_\lambda}^{(\lambda)}\big) = 0$ であり，したがって，$g_\lambda\big(X, \beta_1^{(\lambda)},\ldots, \beta_{n_\lambda}^{(\lambda)}\big) = 0$ である．よって，

$$f_\lambda(X) = \prod_{i=1}^{n_\lambda}\big(X-\beta_i^{(\lambda)}\big)\in L[X] \qquad ①$$

となる．特に $\beta_i^{(\lambda)}$ は K 上代数的である．L は K 上 $\beta_i^{(\lambda)}$ 達で生成されるので，L は K の代数拡大である．

また，$K[X]$ の任意の既約モニック多項式 $f_\lambda(X)$ は ① のように $L[X]$ において 1 次式の積に因数分解できるから，L は代数閉体である．

(2) 定理 4.3(3) の証明のように，一般化した命題 (P) を証明する．

(P) K_1, K_2 は体で同型写像 $\tau\colon K_1\to K_2$ が存在すると仮定する．L_1 は K_1 の代数閉包，L_2 は K_2 の代数閉包とする．すると，同型写像 $\sigma\colon L_1\to L_2$ で $\sigma|_{K_1} = \tau$ を満たすものが存在する．

$$\mathfrak{M} := \left\{(M,\rho) \;\middle|\; \begin{array}{l} M \text{ は } K_1\subset M\subset L_1 \text{ を満たす体で，}\\ \rho\colon M\to L_2 \text{ は中への同型写像で } \rho_{K_1} = \tau \end{array}\right\}$$

とおく．$(M_1,\rho_1), (M_2,\rho_2)\in\mathfrak{M}$ に対して，$M_1\subset M_2$ かつ $\rho_2|_{M_1} = \rho_1$ が成り立つとき $(M_1,\rho_1)\leqq(M_2,\rho_2)$ であるとして $\mathfrak{M}$ に順序を定める．このとき，$\mathfrak{M}$ が帰納的順序集合になることは容易にわかる．Zorn の補題によって，$\mathfrak{M}$ には極大元 (M_0,ρ_0) が存在する．

(iii) $M_0\neq L_1$ と仮定して矛盾を導く．

$c \in L_1 - M_0$ を取り，c の M_0 上の最小多項式を $f_c(X) \in M_0[X]$ とする．また，$M_1 := M_0(c)$ とし，$\rho(f_c(X))$ の L_2 における根の 1 つを d とする．勝手な $y \in M_1$ は，ある $e_0, e_1, \ldots, e_{n-1} \in M_0$ (ただし $n = \deg f_c(X)$) により，$y = e_0 + e_1 c + e_2 c^2 + \cdots + e_{n-1} c^{n-1}$ と書ける．

$$\rho_1(y) = \rho_0(e_0) + \rho_0(e_1)d + \rho_0(e_2)d^2 + \cdots + \rho_0(e_{n-1})d^{n-1} \in L_2$$

により，$\rho_1 \colon M_1 \to L_2$ を定義すると，$(M_1, \rho_1) \in \mathfrak{M}$ で，$(M_0, \rho_0) < (M_1, \rho_1)$ となり，(M_0, ρ_0) の極大性に矛盾する．よって，$M_0 = L_1$ である．

(iv) そこで，$\sigma = \rho_0 \colon L_1 \to L_2$ とおく．$\sigma(L_1) \neq L_2$ と仮定して矛盾を導く．

$d \in L_2 - \sigma(L_1)$ を取り，d の $\sigma(L_1)$ 上の最小多項式を $f_d(X)$ とする．$\deg f_d(X) \geqq 2$ で，$\sigma^{-1}(f_d(X)) \in L_1[X]$ は既約多項式であるが，これは L_1 が代数閉体であることに矛盾する．よって $\sigma(L_1) = L_2$ で，$\sigma \colon L_1 \to L_2$ は同型写像である． □

6. 分離拡大・非分離拡大

K が体 (または可換環) のとき，$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ に対し，

$$\frac{d}{dX} f(X) := n a_n X^{n-1} + (n-1) a_{n-1} X^{n-1} + \cdots + a_1 \in K[X]$$

と定義し，$f(X)$ の**導関数**という．ここで，$k \in \mathbb{Z}$ に対し K を $\mathbb{Z}$-加群と考えて $k a_k \in K$ と考える．誤解の恐れがないときは，$\dfrac{d}{dX} f(X)$ を $f'(X)$ とも書く．多変数関数の偏導関数も同様に定義する (本講義では使わない)．多項式の導関数については，$(f(X)g(X))' = f'(X)g(X) + f(X)g'(X)$ などの通常の微分の公式が成立する．ただし，極限 lim を含むような公式は適用できないし，無限和 $\displaystyle\sum_{n=0}^{\infty}$ を含む公式も適用できない．次の命題は，微分法の公式から簡単に証明できる．

定理 6.1. K は体とし，$f(X) \in K[X]$ は 1 次以上の多項式とする．もし，$f(X)$ が $a \in K$ を m 重根にもつならば，$f(X)$ の導関数 $f'(X)$ は a を $(m-1)$ 重根に持つ．したがって，$\mathrm{GCD}(f(X), f'(X))$ の根が $f(X)$ の重根である．ここで，GCD は最大公約数を表す記号で，多項式について用いる場合，答がモニック多項式になるように選んでおく．

ところで，$f(X) = X^p \in \mathbb{F}_p[X]$ のとき，$f'(X) = pX^{p-1}$ であるが，この係数の p は $p \cdot 1_{\mathbb{F}_p} = 0$ と同一視されるので，$f'(X) = 0$ である．もっと一般に，K が標数 p (p は素数) の体のとき，

$$f(X) = a_n X^{np} + a_{n-1} X^{(n-1)p} + \cdots + a_1 X^p + a_0 \in K[X] \qquad ①$$

に対して $f'(X) = 0$ となる．逆に $f(X) \in K[X]$ が $f'(X) = 0$ を満たせば $f(X)$ は ① のような形であることはすぐわかる．以上をまとめて，

定理 6.2. K は体で，その標数は素数 p であるとする．また，$f(X) \in K[X]$ で $f'(X) = 0$ を満たすとする．すると，ある $g(X) \in K[X]$ により $f(X) = g(X^p)$ と表すことができる．逆に $f(X) = g(X^p)$ と書ければ $f'(X) = 0$ である．

定義 6.3. K は体，L は K の代数拡大体であるとする．$c \in L$ に対し K 上の c の最小多項式を $f_c(X) \in K[X]$ とする．もし，$f_c(X)$ が重根を持たないならば c は K 上**分離的** (separable) であるといい，もし，$f_c(X)$ が重根を持つならば c は K 上**非分離的** (inseparable) であるという．また，$f_c(X) = (X-c)^n$ $(\exists n \in \mathbb{N})$ と書けるとき，c は K 上**純非分離的**であるという．(後で示すが，このとき $f_c(X) = (X-c)^{p^e}$ という形になる.)

L のすべての元が K 上分離的であるとき L は K の**分離** (的) 拡大であるとか，L は K 上**分離的**であるという．そうでないとき，L は K の**非分離** (的) 拡大であるとか，L は K 上**非分離的**であるという．K に属さない L のすべての元が K 上純非分離的であるとき，L は K の**純非分離** (的) 拡大であるとか，L は K 上**純非分離的**であるという．$L = K$ の場合も L は K 上純非分離的であるという．

例 6.4. 純非分理拡大の例を 1 つ構成する．p は素数として，T を不定元 ($\mathbb{F}_p$ 上超越的な元) として，$K = \mathbb{F}_p(T)$, $L = \mathbb{F}_p(T^{1/p})$ とおく．$L = K(T^{1/p})$ で $T^{1/p}$ の K 上の最小多項式 $f(X) \in K[X]$ は，

$f(X) = X^p - T$ である．$L[X]$ においては $f(X) = (X - T^{1/p})^p$ なので，$T^{1/p}$ は K 上純非分離的である．$L = K[X]/(f(X)) = K[T^{1/p}]$ でもあるので，L の元 y はある $g(X) \in K[X]$ により $y = g(T^{1/p})$ と書ける．g の係数 $c \in F_p$ は $c^p = c$ を満たすので，$(X - g(T^{1/p}))^p = X^p - (g(T^{1/p}))^p = X^p - g(T)$ となる．よって，$y \in L - K$ ならば y の K 上の最小多項式 $f_y(X)$ は $f_y(X) = X^p - g(T)$ で $L[X]$ では $f_y(X) = (X - g(T^{1/p}))^p$ となる．よって，y は K 上純非分離的である．したがって，L は K の純非分離拡大である．

定義 6.5. K は体とする．K の任意の代数拡大体 L が K 上分離的であるとき，K は**完全体** (perfect field) であるという．$\overline{K}$ を K の代数閉包とする．もし，任意の元 $a \in \overline{K}$ が K 上分離的ならは K は完全体である．よって，任意の K の有限次代数拡大体 $K(a)$ が K 上分離的ならば，K は完全体である．

定理 6.6. 標数 0 の体 K は完全体である．

証明. K の非分離的代数拡大体 L が存在して，$c \in L$ が K 上非分離的であったとする．c の K 上の最小多項式を $f_c(X) \in K[X]$ とする．K の標数は 0 だから $f_c'(X) \neq 0$ である．$f_c(X)$ は $(X - c)^2$ の倍数だから $f_c'(X)$ は $X - c$ の倍数で，$f_c'(c) = 0$ である．これは $f(X)$ が最小多項式であることに矛盾する． □

命題 6.7. K は体，L は K の代数拡大体で，$c \in L$ は K 上純非分離的であるとする．すると，K の標数 p は素数で，c の K 上の最小多項式 $f_c(X)$ はある自然数 $e \in \mathbb{N}$ により，$f_c(X) = (X - c)^{p^e}$ と書ける．

証明. 前定理の証明のように，$f_c(X) = (X - c)^n$ が重根を持つならば，$f_c'(X) = 0$ でなければならない．よって，ある $g(X) \in K[X]$ により $f_c(X) = g(X^p)$ と書ける．特に，n は p の倍数で，$n = mp$ $(\exists m \in \mathbb{N})$ と書ける．$f_c(X) = (X - c)^{pm} = ((X - c)^p)^m = (X^p - c^p)^m$ なので，$g(X) = (X - c^p)^m$ である．これは c^p の K 上最小多項式であるから，同じ理由で m は p の倍数である．この操作を繰り返していけば，$n = p^e$ と書けることがわかる． □

定理 6.8. 体 K の標数は素数 p であるとする．K が完全体であるための必要十分条件は，任意の $a \in K$ に対して $b^p = a$ を満たす $b \in K$ が存在することである．

証明. K の代数閉包 L を取る．

(必要性) $a \in K$ に対して $b^p = a$ となる $b \in L$ を取ると，$(X - b)^p = X^p - b^p = X^p - a$ なので，$b \in L$ の K 上の最小多項式 $f_b(X) \in K[X]$ は $L[X]$ において $(X - b)^p$ の約数である．よって，$f_b(X) = (X - b)^n$ $(1 \leqq n \leqq p)$ と書ける．$b \notin K$ とすると，$n \neq 1$ であるが，これは K が完全体であることに矛盾する．

(十分性) 任意の $a \in K$ に対して $b^p = a$ を満たす $b \in K$ が存在するが，K は完全体でないと仮定して矛盾を導く．K は完全体でないから，ある非分離的な $b \in L - K$ が存在する．b の K 上の最小多項式 $f_b(X) \in K[X]$ は $f_b'(X) = 0$ を満たす．よって，ある $g(X) \in K[X]$ により $f_b(X) = g(X^p)$ と書ける．$g(X) = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ とし，$b_i^p = a_i$ $(i = 0, \ldots, n)$ を満たす $b_i \in K$ を取る．$h(X) = b_n X^n + \cdots + b_1 X + b_0 \in K[X]$ とおくと，

$$\big(h(X)\big)^n = b_n^p X^{np} + \cdots + b_1^p X^p + b_0^p = g(X^p) = f_b(X)$$

となる．これは，$f_b(X)$ が $K[X]$ で既約であることに矛盾する． □

定理 6.9. 有限体は完全体である．

証明. K は標数 p の有限体とし，K の任意の有限次代数拡大体 L を取る．L も有限体である．$\#L = n$ とするとき，L の任意の元は $f(X) = X^n - X$ の根である．$f(X) = X^n - X$ は $f'(X) = -1 \neq 0$ なので重根を持たない．よって，L は K 上分離的であり，K は完全体である． □

7. 単純拡大

定義 7.1. K は体，L は K の拡大体，Ω は L の代数閉包とする．ある $a \in L$ により $L = K(a)$ と書けるとき，L は K の**単純拡大**であるとか**単項拡大**であるという．

M も K の拡大体であるとき，

$$\mathrm{Mon}_K(L, M) := \left\{\sigma\colon L \to M \;\middle|\; \sigma \text{ は中への同型写像で } \sigma|_K = \mathrm{id}_K\right\}$$

と書くことにする．$\mathrm{Mon}_K(L,\, L) = \mathrm{Aut}(L/K)$ である．

補題 7.2. K は体，L は K の有限次代数拡大体で，ある $a \in L$ により $L = K(a)$ と書けると仮定する．Ω は L の代数閉包とする．a の K 上の最小多項式を $f_a(X) \in K[X]$ とし，$f_a(X)$ の Ω での根全体を $a_1,\ldots,\, a_m$ とおく．このとき，以下が成り立つ．

(1) $\#\,\mathrm{Mon}_K(L,\, \Omega) = m$ が成り立つ．

(2) a が K 上分離的であるための必要十分条件は，$\#\,\mathrm{Mon}_K(L,\, \Omega) = [L : K]$ が成り立つことである．

証明. (1) $\deg f_a(X) = n$ とする．$L = K(a)$ だから，$L = K + Ka + Ka^2 + \cdots + Ka^{n-1}$ であり，$[L : K] = n$ である．各 $1 \leqq i \leqq m$ に致し，$\sigma_i \in \mathrm{Mon}_K(K(a),\, K(a_i))$ を $\sigma_i(a) = a_i$ を満たすものとする．そのような σ_i は一意的に存在する．

勝手な $\tau \in \mathrm{Mon}_K(L,\, \Omega)$ を取る．$f_a(\tau(a)) = \tau(f_a(a)) = 0$ だから，$\tau(a) = a_i$ を満たす $1 \leqq i \leqq m$ が存在する．L の元 y は $y = c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1}a^{n-1}$ $(\exists a_1,\ldots,\, \exists a_{n-1} \in K)$ と書ける．$\tau(c_j) = c_j$, $\tau(a^j) = a_i^j$ だから，

$$\tau(y) = c_0 + c_1 a_i + c_2 a_i^2 + \cdots + c_{n-1} a_i^{n-1} = \sigma_i(y)$$

となり，$\tau = \sigma_i$ となる．よって，$\mathrm{Mon}_K(L,\, \Omega) = \left\{\sigma_1,\ldots,\, \sigma_m\right\}$ である．

(2) a が K 上分離的ならば，上の議論で，$m = n$ である．よって，$\#\,\mathrm{Mon}_K(L,\, \Omega) = m = n = [L : K]$ である．

また，a が K 上非分離的ならば，$m < n$ だから，$\#\,\mathrm{Mon}_K(L,\, \Omega) = m < n = [L : K]$ である． □

補題 7.3. K は体，L は K の有限次代数拡大体で，ある K 上分離的な $a,\, b \in L$ により $L = K(a,\, b)$ と書けると仮定する．すると，ある $c \in L$ が存在して $L = K(c)$ と書ける．また，$L = K(c)$ を満たす $c \in L$ は K 上分離的である．

証明. (1) K が有限体の場合．

L も有限体である．$L^\times$ は巡回群なので，その生成元 (原始根) c を取る．すると，$L = K(c)$ である．

(2) K が無限体の場合．

$a,\, b$ の K 上の最小多項式を $f_a(X),\, f_b(X) \in K[X]$ とおく．L の代数閉包 Ω における $f_a(X),\, f_b(X)$ の根全体をそれぞれ $a_1,\ldots\, a_m$ $(m = \deg f_a(X))$, $b_1,\ldots\, b_n$ $(n = \deg f_b(X))$ とおく．$a_1 = a$, $b_1 = b$ と仮定してよい．有限集合

$$\left\{ \frac{b_i - b_j}{a_k - a_l} \in \Omega \;\middle|\; k \neq l \in \{1,\ldots,\, m\}.\ i,\, j \in \{1,\ldots,\, n\} \right\}$$

に含まれない K の元 e を取り，$c = ae + b \in L$ とおく．$g(X) := f_b(c - eX) \in K(c)[X]$ とおくと，$g(a) = f_b(c - ae) = f_b(b) = 0.$ である．$c/e = a + b/e = a_1 + b_1/e$ だから，

$$g(X) = f_b(c - eX) = \prod_{i=1}^{n} \big((c - eX) - b_i\big) = (-e)^n \prod_{i=1}^{n} \left(X - a_1 - \frac{b_1 - b_i}{e} \right)$$

である．e の選び方から $i \geqq 2$ のとき．$a_1 + (b_1 - b_i)/e = a_j$ $(1 \leqq \exists j \leqq m)$ となることはない．よって，$\mathrm{GCD}(f_a(X),\, g(X)) = X - a$ である．$f_a(X),\, g(X) \in K(c)[X]$ だから，その最大公約数も $X - a \in K(c)[X]$ となる．つまり，$a \in K(c),\, b = c - ae \in K(c)$ である．よって，$L = K(a,\, b) \subset K(c)$ である．$c \in L$ であったから $L = K(c)$ となる．

(3) $L = K(c)$ を満たす $c \in L$ は K 上分離的であることを示す．

有限体は完全体であったから，K が無限体の場合に示せばよい．(2) の記号を用いる．

$\sigma_i'(a) = a_i$ で定まる同型写像を $\sigma_i'\colon K(a) \longrightarrow K(a_i)$ とすると，$\mathrm{Mon}_K(K(a),\, \Omega) = \left\{\sigma_1',\ldots,\, \sigma_m'\right\}$ である．$\sigma_i \in \mathrm{Mon}_K(L,\, \Omega)$ で $\sigma_i|_{K(a)} = \sigma_i'$ を満たすものが存在する．各 $1 \leqq i \leqq m$ に対し，そのような σ_i を 1 つずつ選んでおく．ただし，$\sigma_1 = \mathrm{id}_L$ となるように選ぶ．b の $K(a)$ 上の最小多項式を

$g_b(X) \in K(a)[X]$ とおくと，$g_b(X)$ は $f_b(X)$ の約数だから重根を持たず，b は $K(a)$ 上分離的である．$l := \deg g_b(X) = [L : K(a)]$ とし，$g_b(X)$ の根は $b_1, \ldots b_l \in \Omega$ $(b_1 = b)$ であるとしてよい．$K(a_i, \sigma_i(b)) = \sigma_i(L)$ である．$1 \leqq i \leqq m$, $1 \leqq j \leqq l$ に対し $\tau_{i,j} \in \mathrm{Mon}_{K(a_i)}\left(\sigma_i(L), \Omega\right)$ を，$\tau_{i,j}(\sigma_i(b)) = \sigma_i(b_j)$ で定める．$\sigma_i(b)$ は $K(a_i)$ 上分離的だから，$\#\,\mathrm{Mon}_{K(a_i)}\left(\sigma_i(L), \Omega\right) = [\sigma_i(L) : K(a_i)] = [L : K(a)] = l$ であって，$\mathrm{Mon}_{K(a_i)}\left(\sigma_i(L), \Omega\right) = \left\{\tau_{i,1}, \ldots, \tau_{i,l}\right\}$ となる．よって，

$$\mathrm{Mon}_K(L, \Omega) \supset \left\{\tau_{i,j} \circ \sigma_i \;\middle|\; 1 \leqq i \leqq m, 1 \leqq j \leqq l\right\} \qquad ①$$

である．$\tau_{i,j} \circ \sigma_i = \tau_{k,l} \circ \sigma_k$ ならば $(i, j) = (k, l)$ を示そう．$a_i = \tau_{i,j}(a_i) = \tau_{i,j}(\sigma_i(a)) = \tau_{k,l}(\sigma_k(a)) = \tau_{k,j}(a_k) = a_k$ より，$i = k$ である．$\sigma_i(b_j) = \tau_{i,j}(\sigma_i(b)) = \tau_{i,l}(\sigma_i(b)) = \sigma_i(b_l)$ より，$j = l$ となる．したがって，

$$\#\,\mathrm{Mon}_K(L, \Omega) \geqq ml = [K(a) : K] \cdot [L : K(a)] = [L : K] = [K(c) : K]$$

となる．前補題より $\leqq$ なので，$\#\,\mathrm{Mon}_K(L, \Omega) = [K(c) : K]$ となる．よって，c は K 上分離的である． □

定理 7.4. K は体，L は K の有限次代数拡大体とする．また，L の代数閉包を Ω とする．このとき，以下の (1) 〜 (4) は同値である．

(1) L は K 上分離的である．
(2) 何個かの K 上分離的な元 $a_1, \ldots, a_n \in L$ が存在して，$L = K(a_1, \ldots, a_n)$ と書ける．
(3) K 上分離的な元 a が存在して，$L = K(a)$ と書ける．
(4) $\#\,\mathrm{Mon}_K(L, \Omega) = [L : K]$.

証明. (1) $\Longrightarrow$ (2) は自明.
(2) $\Longrightarrow$ (3) は，補題 7.3 を用いて，n に関する帰納法で容易に証明できる．
(3) $\Longrightarrow$ (4) は，補題 7.2 で証明した．

(4) $\Longrightarrow$ (1) を背理法で示す.
$b \in L$ は K 上非分離的とする．L は K 上有限生成だから，ある $a_1, \ldots, a_n \in L$ により，$L = K(b, a_1, \ldots, a_n)$ と書ける．$\#\,\mathrm{Mon}_K(L, \Omega) < [L : K]$ であることを，n に関する帰納法で示す.
$n = 0$，つまり $L = K(b)$ の場合は補題 7.2 で証明した.
$n \geqq 1$, $M := K(b, a_1, \ldots, a_{n-1})$ とし，$\#\,\mathrm{Mon}_K(M, \Omega) < [M : K]$ を仮定する．$\sigma \in \mathrm{Mon}_K(L, \Omega)$ に対し $\sigma|_M \in \mathrm{Mon}_K(M, \Omega)$ である．また，

$$\#\,\mathrm{Mon}_M(M(\sigma(a_n)), \Omega) = \#\,\mathrm{Mon}_M(M(a_n), \Omega) = \mathrm{Mon}_M(L, \Omega) \leqq [L : M]$$

である．補題 7.3 の証明の (3) の部分の考察と同様にして，

$$\#\,\mathrm{Mon}_K(L, \Omega) \leqq \#\,\mathrm{Mon}_K(M, \Omega) \times \#\,\mathrm{Mon}_M(L, \Omega) < [M : K] \cdot [L : M] = [L : K]$$

がわかる． □

定理 7.5. K は体，L は K の代数拡大体とする．

$$K_L^s := \left\{a \in L \;\middle|\; a \text{ は } K \text{ 上分離的}\right\}$$

とおくと，K_L^s は K の分離拡大体，L は K_L^s の純非分離拡大体になる．

証明. (1) K_L^s が体であることを示す．$0 \neq a, b \in K_L^s$ に対し，前定理より $K(a, b)$ は K 上分離的である．よって，$a + b$, ab, $1/a$ も K 上分離的である．したがって $a + b$, ab, $1/a \in K_L^s$ で，K_L^s は体である．
K_L^s は K の分離拡大であることは自明.

(2) L は K_L^s の純非分離拡大であることを示す.
K の標数を p とし，$c \in L - K_L^s$ の K 上の最小多項式を $f_c(X) \in K[X]$ とする．$f_c(X)$ は重根を持つから，ある $g_1(X) \in K[X]$ により $f_c(X) = g_1(X^p)$ と書ける．もし $g_1(X)$ も重根を持てば，ある $g_2(X) \in K[X]$ により $g_1(X) = g_2(X^p)$ と書ける．以下，帰納的に $g_i(X) = g_{i+1}(X^p)$ を満たす $g_{i+1}(X) \in K[X]$ を取ることを繰り替えすと，ある $e \in \mathbb{N}$ のところで $g_e(X)$ は重根を持たなくなる (次数が有限だから)．すると，$f(X) = g_e(X^{p^e})$ と書ける．c^{p^e} の最小多項式は $g_e(X)$ で，これは重根を持たないから $c^{p^e} \in K_L^s$ である．つまり，c の K_L^s 上の最小多項式は $X^{p^e} - c^{p^e} = (X - c)^{p^e}$ であり，c は K_L^s 上純非分離的である． □

定義 7.6. 上定理の K_L^s を K の L における**分離閉包**という．$[K_L^s : K]$ を L の K 上の**分離次数**といい，$[L : K_L^s]$ を L の K 上の**非分離次数**という．

定理 7.7. K は体，L は K の有限次代数拡大体で，Ω は L の代数閉包とする．$\#\operatorname{Mon}_K(L, \Omega) = [K_L^s : K]$ (分離次数) が成り立つ．

証明. 補題 7.2 からすぐわかる． □

定理 7.8. K は体 $L = K(a)$ が K の有限次代数拡大体ならば．K と L の中間体の個数は有限である．

証明. $\mathfrak{M} := \{M \mid M \text{ は } K \text{ と } L \text{ の中間体 }\}$ とおく．a の K 上の最小多項式を $f(X) \in K[X]$ とする．$M \in \mathfrak{M}$ を取り，a の M 上の最小多項式を $f_M(X) \in M[X]$ とする．$f_M(X)$ は $f(X)$ の約数である．$f(X)$ の約数は有限個しかない．

$f_M(X) = f_N(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ $(c_i \in M \cap N)$ とする．ここで $n = [L : M]$ である．$F := K(c_0, \ldots, c_{n-1})$ とおく．$F \subset M$ である．$f_M(X) \in F[X]$ なので，F 上の a の最小多項式も $f_M(X)$ である．よって，$[L : F] = \deg f_M(X) = n = [L : M]$ なので，$F = M$ となる．

$N \in \mathfrak{M}$ が $f_N(X) = f_M(X)$ を満たせば，今の考察から $N = F = M$ となる．よって，$\#\mathfrak{M}$ は $f(X)$ の約数の個数以下である． □

8. 正規拡大・ガロア拡大

定義 8.1. K は体とする．L が K の**正規拡大**であるとか，L が K の代数拡大体であって，任意の $a \in L$ に対し，a の K 上の最小多項式を $f_a(X) \in K[X]$ とするとき $L[X]$ において $f_a(X)$ が 1 次式の積に因数分解できることをいう．

L が K の正規拡大であって分離拡大であるとき，L は K の**ガロア拡大**とか **Galois 拡大**であるという．L が K のガロア拡大のとき，$\operatorname{Aut}(L/K)$ を $\operatorname{Gal}(L/K)$ とか $\mathrm{G}(L/K)$ とも書き**ガロア群**という．$\operatorname{Gal}(L/K)$ という記号は，暗に L が K のガロア拡大であることを仮定しているときに用いる．

定理 8.2. K は体，$L = K(a_1, \ldots, a_n)$ は K の有限次代数拡大体とする．

(1) L が K の正規拡大であるための必要十分条件は，各 $i = 1, \ldots, n$ に対し a_i のすべての共役元が L に属することである．
(2) L が K の正規拡大ならば，Ω を L の代数閉包とするとき $\operatorname{Mon}_K(L, \Omega) = \operatorname{Gal}(L/K)$ である．
(3) L が K の有限次正規拡大ならば，L 内での K の分離閉包を K_L^s とするとき，$\operatorname{Aut}(L/K) \cong \operatorname{Gal}(K_L^s/K)$ である．
(4) L が K の有限次正規拡大ならば，$a \in L$ の K 上の共役元全体は $\{\sigma(a) \mid \sigma \in \operatorname{Aut}(L/K)\}$ である．

証明. (1) 必要性は自明．十分性を示す．$a_1, \ldots, a_n$ のすべての共役元が L に属するとする．a_i の K 上の最小多項式を $f_i(X) \in K[X]$ とする．$f(X) = f_1(X) \cdots f_n(X)$ とおくと，L は $f(X)$ の最小分解体である．

勝手な $b \in L$ と，その K 上の共役 $b' \in \Omega$ を取る．ある $\sigma \in \operatorname{Mon}_K(L, \Omega)$ により $b' = \sigma(b)$ と書ける．$\sigma(f(X)) = f(X)$ だから，$\sigma(L)$ も $f(X)$ の最小分解体である．最小分解体の一意性から $\sigma(L) = L$ となり，$\sigma \in \operatorname{Aut}(L/K)$ となる．特に，$b' = \sigma(b) \in L$ である．よって，L は K の正規拡大である．

(2) と (4) は上の証明の中で示されている．

(3) は補題 7.2 から得られる． □

定理&定義 8.3. L は体，P は L 内の素体とする．$G \subset \operatorname{Aut}(L/P)$ は有限部分群とし．

$$K = L^G := \{a \in G \mid \text{任意の } \sigma \in G \text{ に対して } \sigma(b) = b\}$$

とおく．L^G を G による L の**不変部分体**という．このとき，L は K のガロア拡大で，$G = \operatorname{Gal}(L/K)$ が成り立つ．

証明. 勝手な $a \in L$ に対し $H_a := \{\sigma \in G \mid \sigma(a) = a\}$ とし，$H_a \backslash G := \{H_a\tau \mid \tau \in G\}$ の完全代表系を $\tau_1, \ldots, \tau_r$ とする．ここで，$r = |G/H_a| = \#G/\#H_a$ である．$a_i = \tau_i(a)$ とおくと，$a_1, \ldots, a_r$ が相異

なる a のすべての L 内の共役元である．

$$f_a(X) = (X - a_1)\cdots(X - a_r) = X^r + c_1X^{r-1} + \cdots + c_{r-1}X + c_r$$

とおく．c_i は i 次の $a_1,\ldots, a_r$ の基本対称式の $(-1)^i$ 倍であるので，$\tau_j(c_i) = c_i$ が成り立つ．任意の $\sigma \in H_1$ に対して $\sigma(c_i) = c_i$ を満たすから，任意の $\sigma \in G$ に対して $\sigma(c_i) = c_i$ を満たす．$K = L^G$ なので $c_i \in K$ である．$f_a(a) = 0$ で $f_a(X) \in K[X]$ だから，a の K 上の最小多項式は $f_a(X)$ の約数であるが，$f_a(X)$ の根 a_j は a の K 上の共役だから，$f_a(X)$ が K 上の最小多項式になる．また，a の K 上の共役元は $a_1,\ldots, a_r$ 以外にない．勝手な $a \in L$ の K 上のすべての共役元が L に含まれるから，L は K の正規拡大である．$f_a(X)$ は重根を持たないから a は K 上分離的である．よって，L は K の分離拡大であり，L は K のガロア拡大である．

あと，$G = \mathrm{Gal}(L/K)$ を示せばよい．

今 $[K(a) : K]$ を最大にするような $a \in L$ を取る．上の考察から $[K(a) : K] = \deg f_a(X) \leqq \#G$ である．もし $\exists b \in L - K(a)$ ならば，$[K(a,b) : K] > [K(a) : K]$ である．a, b は K 上分離的だから，定理 7.4 より，ある $c \in L$ により $K(a,b) = K(c)$ と書ける．$[K(c) : K] > [K(a) : K]$ で，これは $[K(a) : K]$ の最大性に矛盾する．したがって，$K(a) = L$ である．特に，$[L : K] \leqq \#G$ である．他方，$G \subset \mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ だから，$\#G \leqq \#\,\mathrm{Gal}(L/K) = [L : K]$ である．よって，$\#G = \#\,\mathrm{Gal}(L/K)$ で，$G = \mathrm{Gal}(L/K)$ となる． □

定理 8.4. L は K の有限次正規拡大体とする．K_L^s は L 内での K の分離閉包とする．また，

$$K_L^i := \left\{a \in L \;\middle|\; a \text{ は } K \text{ 上純非分離的であるか，または } a \in K\right\}$$

とおく．さらに，$G := \mathrm{Aut}(L/K)$ とおく．このとき，以下が成り立つ．

(1) K_L^i は体であり，$K_L^i = L^G$ が成り立つ．

(2) L は K_L^i のガロア拡大で，$\mathrm{Gal}(L/K_L^i) = \mathrm{Aut}(L/K)$.

(3) $[L : K_L^i] = [K_L^s : K]$, $[L : K_L^s] = [K_L^i : K]$.

(4) L は $K_L^s \cup K_L^i$ を含む最小の体である．

証明. (1) $G := \mathrm{Aut}(L/K)$ とし，$F := L^G$ とおく．前定理より，L は F のガロア拡大で，$G = \mathrm{Gal}(L/F)$ である．

(i) $F \subset K_L^i$ を示す．

$\exists a \in F - K_L^i$ と仮定する．a は K 上純非分離的でないから，a の K 上の最小多項式 $f_a(X) \in K[X]$ は L 内に a 以外の根 $b \in L$ を持つ．$\sigma(a) = b$ を満たす $\sigma \in G$ が存在する．これは $a \in L^G$ であることに矛盾する．よって，$F \subset K_L^i$ である．

(ii) 逆に $a \in K_L^i$ ならば，$f_a(X)$ は a 以外の根を持たないから，任意の $\sigma \in G$ に対して $\sigma(a) = a$ となるから，$a \in L^G = F$ で $K_L^i \subset F$ である．以上より $K_L^i = F$ であり，K_L^i は体である．

(2) は (1) と前定理からわかる．

(3) 上結果と定理 8.2(3) より，$\mathrm{Gal}(L/K_L^i) = \mathrm{Aut}(L/K) \cong \mathrm{Gal}(K_L^s/K)$ である．よって，$[L : K_L^i] = [K_L^s : K]$ である．また，

$$[L : K_L^s] = \frac{[L : K]}{[K_L^s : K]} = \frac{[L : K]}{[L : K_L^i]} = [K_L^i : K]$$

である．

(4) $K_L^s \cup K_L^i$ を含む L の最小の部分体を L_0 とする．L は K_L^s の純非分離拡大だから，L は L_0 の純非分離的拡大である．L は K_L^i の分離拡大だから，L は L_0 の分離的拡大である．よって，$L_0 = L$ である． □

定義 8.5. Ω は体で，K と L は Ω の部分体であるとする．Ω の中で $K \cup L$ を含む最小の部分体を KL と書き，K と L で**生成される体**という．KL の元 x は，ある $n \in \mathbb{N}$ と，ある $a_1,\ldots, a_n \in K$ と，ある $b_1,\ldots, b_n \in L$ により，$x = a_1b_1 + \cdots + a_nb_n$ と書ける．KL を $K(L)$ とか $L(K)$ と表すこともできる．また，$K \cap L$ は (素体を含む) 体である．

定理 8.6. K は体，Ω は K の代数閉包で，体 L, M は $K \subset L \subset \Omega$, $K \subset M \subset \Omega$ を満たすとする．L が K の有限次ガロア拡大ならば，LM は M の有限次ガロア拡大で，

$$\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/(L \cap M)), \quad [LM : M] = [L : (L \cap M)]$$

が成り立つ．

証明. 定理 8.2 より L は $L\cap M$ の有限次ガロア拡大でもあるので，$K=L\cap M$ の場合に証明すれば十分である．ある $a\in L$ により $L=K(a)$ と書ける．a の K 上の最小多項式を $f_a(X)$ とし，$f_a(X)$ の根全体を $a_1,\ldots, a_n\in L$ ($n=\deg f_a(X)=[L:K]$ とする．a の M 上の共役元は $a_1,\ldots, a_n$ の中に含まれる．必要なら添え字を付け替えて $a_1,\ldots, a_r$ が a の M 上の共役元全体であると仮定してよい．$LM=M(L)=M(K(a))=M(a)$ で，$a_1,\ldots, a_n\in L\subset M(a)$ なので，ML は M の有限次ガロア拡大である．$g(X):=(X-a_1)\cdots(X-a_r)$ とおくと，$g(X)$ が a の M 上の最小多項式である．$g(X)$ は $f_a(X)$ の約数である．$g(X)$ の X^i の係数は $a_1,\ldots, a_r$ の i 次の基本対称式の $(-1)^i$ 倍であるので $L\cap M=K$ に含まれる．つまり $g(X)\in K[X]$, $g(a)=0$ で，$f_a(X)\in K[X]$ は $f_a(a)=0$ を満たす $K[X]$ 内の次数最小のモニック多項式であったから，$g(X)=f_a(X)$ となる．よって，$[LM:M]=\deg g(X)=\deg f_a(X)=[L:K]$ となる．

$\sigma\in\mathrm{Gal}(LM/M)$ を取る．$x\in L$ は $x=c_0+c_1a+c_2a^2+\cdots+c_{n-1}a^{n-1}$ ($c_0,\ldots, c_{n-1}\in K$) と書けるが，$\sigma(a)=a_i$ とすると，$\sigma(x)=c_0+c_1a_i+c_2a_i^2+\cdots+c_{n-1}a_i^{n-1}\in L$ となる．よって，$\sigma|_L\in\mathrm{Gal}(L/K)$ である．$\varphi\colon\mathrm{Gal}(LM/M)\longrightarrow\mathrm{Gal}(L/K)$ を $\varphi(\sigma)=\sigma|_L$ で定める．φ が群の準同型写像であることはすぐわかる．$\tau\in\mathrm{Gal}(L/K)$ が $\tau(a)=a_i$ を満たすとする．$x\in LM=M(a)$ は $x=b_0+b_1a+b_2a^2+\cdots+b_{n-1}a^{n-1}$ ($c_0,\ldots, c_{n-1}\in M$) と書けるが，$\sigma(x)=b_0+b_1a_i+b_2a_i^2+\cdots+b_{n-1}a_i^{n-1}\in L$ で定まる $\sigma\in\mathrm{Gal}(LM/M)$ を取れば $\varphi(\sigma)=\tau$ となる．よって，φ は全射である．また，$\sigma\neq\sigma'\in\mathrm{Gal}(LM/M)$ ならば $\sigma(a)\neq\sigma'(a)$ なので，φ は単射である．よって，φ は同型写像である． □

9. ガロア理論の基本定理

K は体，L は K の代数拡大体とする．今 K と L の中間体全体の集合を

$$\mathfrak{M}(L/K):=\big\{M\;\big|\;M\text{ は }K\text{ と }L\text{ の中間体}\big\}$$

と書くことにする．L が K の正規拡大である場合に，$M\in\mathfrak{M}(L/K)$ に対し，

$$H(M):=\big\{\sigma\in\mathrm{Aut}(L/K)\;\big|\;\text{任意の }x\in M\text{ に対して }\sigma(x)=x\big\}$$

とおく．また，$\mathrm{Aut}(L/K)$ の部分群全体の集合を

$$\mathfrak{H}(L/K):=\big\{H\;\big|\;H\text{ は }\mathrm{Aut}(L/K)\text{ の部分群}\big\}$$

と書くことにする．

さらに，一般に群 G について，H が G の正規部分群であるとき，$G\rhd H$ とか $H\lhd G$ と書くことにする．

定理 9.1.(ガロアの基本定理) K は体，L は K の有限次ガロア拡大であるとする．写像 $\Phi:\mathfrak{M}(L/K)\longrightarrow\mathfrak{H}(L/K)$ を $\Phi(M)=H(M)$ で定める．このとき，以下が成り立つ．

(1) $\Phi:\mathfrak{M}(L/K)\longrightarrow\mathfrak{H}(L/K)$ は全単射で，その逆写像は $H\in\mathfrak{H}(L/K)$ に対し $\Phi^{-1}(H)=L^H\in\mathfrak{M}(L/K)$ で与えられる．また，$\Phi(M)=\mathrm{Gal}(L/M)$ である．

(2) $M\in\mathfrak{M}(L/K)$ に対し，M が K のガロア拡大であるための必要十分条件は $H(M)$ が G の正規部分群であることである．

(3) $M\in\mathfrak{M}(L/K)$ が K の正規拡大であるとき，$\mathrm{Gal}(M/K)=\mathrm{Gal}(L/K)/H(M)$ が成り立つ．

(4) M_1, $M_2\in\mathfrak{M}(L/K)$ に対して，以下が成り立つ．

(4-1) $M_1\subset M_2\Longleftrightarrow H(M_1)\supset H(M_2)$.

(4-2) $H(M_1M_2)=H(M_1)\cap H(M_2)$.

(4-3) $H(M_1\cap M_2)$ は $H(M_1)\cup H(M_2)$ で生成される $\mathrm{Gal}(L/K)$ の部分群と一致する．

(4-4) $\sigma\in\mathrm{Gal}(L/K)$ に対し，$H(\sigma(M))=\sigma^{-1}H(M)\sigma$ である．

証明. (1) $\Psi:\mathfrak{H}(L/K)\longrightarrow\mathfrak{M}(L/K)$ を $\Psi(H)=L^G$ で定める．$M\in\mathfrak{M}(L/K)$ を取る．L は M のガロア拡大だから，定理 8.2 より $\Phi(M)=H(M)=\mathrm{Gal}(L/M)$ が成り立つ．また，$\Psi(\Phi(M))=\Psi(H(M))=L^{H(M)}=M$ である．

同様に，定理 8.2 より，$H\in\mathfrak{H}(L/K)$ に対して $H=\mathrm{Gal}(L/L^H)=H(L^H)=\Phi(L^H)=\Phi(\Psi(H))$ が成り立つ．よって，$\Psi=\Phi^{-1}$ で Φ は全単射である．

(2) M が K のガロア拡大ならば，$a \in M$ の K 上の共役元は M に属するから，任意の $\sigma \in \mathrm{Gal}(L/K)$ に対し $\sigma(M) = M$ である．その逆も成り立つ．任意の $\tau \in H(M)$ は $\tau|_M = \mathrm{id}_M$ を満たすから，$(\sigma^{-1}\tau\sigma)|_M = \mathrm{id}_M$ であり，$\sigma^{-1}\tau\sigma \in H(M)$ である．よって，$H(M) \lhd \mathrm{Gal}(L/K)$ である．逆に，$H(M) \lhd \mathrm{Gal}(L/K)$ ならば，$\sigma^{-1}\tau\sigma \in H(M)$ から $\sigma(M) = M$ が得られるので，M は K のガロア拡大である

(3) $M \in \mathfrak{M}(L/K)$ が K の正規拡大であるとき，上で述べたように $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) = M$ であるから $\sigma|_M \in \mathrm{Gal}(M/K)$ である $\varphi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K)$ を $\varphi(\sigma) = \sigma|_M$ で定めると，これは群の準同型写像である．$L = M(a)$ $(\exists a \in L)$, $m := [L : M]$ とするとき，勝手な元 $x \in L$ は $L = c_0 + c_1 a + c_2 a^2 + \cdots + c_{m-1}a^{m-1}$ $(\exists c_0, \ldots, \exists c_{m-1} \in M)$ と書けるので，$\tau \in \mathrm{Gal}(M/K)$ に対して，$\overline{\tau}(x) = \tau(c_0) + \tau(c_1)a + \tau(c_2)a^2 + \cdots + \tau(c_{m-1})a^m$ で $\overline{\tau}$ を定めれば，$\overline{\tau} \in \mathrm{Gal}(L/K)$ で $\varphi(\overline{\tau}) = \tau$ が成り立つ．よって，φ は全射である．定義から $\mathrm{Ker}\,\varphi = H(M)$ であるので，準同型定理により $\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/H(M)$ が成り立つ．

(4-1) は自明.

(4-2) $H(M_1M_2) \subset H(M_1)$, $H(M_1M_2) \subset H(M_2)$ は自明だから，$H(M_1M_2) \subset H(M_1) \cap H(M_2)$ である．$\supset$ を示す．$\sigma \in H(M_1) \cap H(M_2)$ とする．M_1M_2 の元は $z = x_1y_1 + \cdots + x_ky_k$ $(x_i \in M_1, y_i \in M_2)$ という形に書ける．$\sigma \in H(M_1)$ より $\sigma(x_i) = x_i$, $\sigma \in H(M_2)$ より $\sigma(y_i) = y_i$ なので，$\sigma(z) = z$ が得られる．よって，$\sigma \in M(M_1M_2)$ で，$H(M_1M_2) = H(M_1) \cap H(M_2)$ である．

(4-3) $H(M_1) \cup H(M_2)$ で生成される $\mathrm{Gal}(L/K)$ の部分群を H' とする．$H(M_1 \cap M_2) \supset H(M_1)$, $H(M_1 \cap M_2) \supset H(M_2)$ より $H(M_1 \cap M_2) \supset H'$ である．$\subset$ を示す．$M' := L^{H'}$ とおく．$H' \supset H(M_1)$ より，$M' = L^{H'} \subset L^{H(M_1)} = M_1$ である．よって，$M' \subset M_1 \cap M_2$. 他方 $x \in M_1 \cap M_2$ ならば，任意の $\sigma \in H'$ に対して $\sigma(x) = x$ を満たすから，$x \in L^{H'} = M'$ となる．よって，$M' = M_1 \cap M_2$ である．したがって，$H(M_1 \cap M_2) = H(M') = H'$.

(4-4) $\tau \in H(\sigma(M))$ は，任意の $x \in M$ に対して $\tau(\sigma(x)) = \sigma(x)$ を満たす．よって，$\sigma^{-1}\tau(\sigma(x)) = x$ だから，$x \in \sigma^{-1}H(M)\sigma$ である．つまり，$H(\sigma(M)) \subset \sigma^{-1}H(M)\sigma$ である．同様に，$H(M) \subset \sigma H(\sigma(M))\sigma^{-1}$ も証明できるので，(4-4) を得る． □

定義 9.2. K は体，L は K の有限次ガロア拡大とする．$\mathrm{Gal}(L/K)$ がアーベル群のとき，L は K の**アーベル拡大**であるという．$\mathrm{Gal}(L/K)$ が巡回群のとき，L は K の**巡回拡大**であるという．

定義 9.3.(原始 n 乗根) n は自然数，Ω は代数閉体とし，$G := \left\{x \in \Omega \;\middle|\; x^n = 1\right\}$ とおく．補題 3.8 より G は積 (乗法) について巡回群になる．$x \in G$ が巡回群 G の生成元であるとき，x は **1 の原始 n 乗根**であるという．

$p := \mathrm{char}\,\Omega > 0$ で $n = p^e m$ $(m \in \mathbb{N}$ で $\mathrm{GCD}(m, p) = 1)$ と表せるときは，$X^n - 1 = (X^m - 1)^{p^e}$ なので，1 の原始 n 乗根は 1 の原始 m 乗根である．

定理 9.4. K は体，L は $X^n - 1$ の最小分解体であるとする．すると，L は K のアーベル拡大である．また，K の標数が 0 であるか n と $p := \mathrm{char}\,K > 0$ が互いに素ならば，$\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ である．

証明. $n = p^e m$ の場合は，$X^n - 1 = (X^m - 1)^{p^e}$ だから，$X^n - 1$ が重根を持たない場合に証明すればよい．$\zeta \in L$ を 1 の原始 n 乗根とする．$K(\zeta) \subset L$ であるが，L は $X^n - 1$ の最小分解体だから $L = K(\zeta)$ である．ζ は K 上分離的だから，L は K の分離拡大である．ζ の K 上の共役はすべて L に属するので，L は K の正規拡大であり，有限次ガロア拡大である．$\sigma \in \mathrm{Gal}(L/K)$ に対し $\sigma(\zeta) = \zeta^k$ を満たす $k \in \mathbb{Z}$ が存在するが，k は $(\mathbb{Z}/n\mathbb{Z})^\times$ の元と考えることができる．そこで，$\varphi(\sigma) = k$ によって $\varphi\colon \mathrm{Gal}(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ を定める．

$\tau \in \mathrm{Gal}(L/K)$ が $\sigma(\zeta) = \zeta^l$ を満たすとき，$\tau\sigma(\zeta) = \zeta^{kl}$ なので φ 準同型写像である．$\sigma \neq \tau$ ならば $\zeta^k \neq \zeta^l$ なので φ は単射である．また，$k \in (\mathbb{Z}/n\mathbb{Z})^\times$ ならば ζ^k も 1 の原始 n 乗根であるから，$\sigma(\zeta) = \zeta^k$ から誘導される $\sigma \in \mathrm{Mon}_K(L, \Omega)$ は $\sigma \in \mathrm{Gal}(L/K)$ を満たす．そして，$\varphi(\sigma) = k$ だから，φ は全射である．したがって，$\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ で，L は K のアーベル拡大である． □

補題 9.5. K は体，L は K の代数拡大体，Ω は L の代数閉包とし，$\sigma_1, \ldots, \sigma \in \mathrm{Mon}_K(L, \Omega)$ は相異なる中への同型写像とする．また，$c_1, \ldots, c_n \in \Omega - \{0\}$ とする．このとき，ある $a \in L$ で，$\displaystyle\sum_{i=1}^{n} c_i\sigma_i(a) \neq 0$

を満たすものが存在する．

証明. $x \in L$ に対し $\varphi(x) := \sum_{i=1}^{n} c_i\sigma_i(x) \in \Omega$ として，写像 $\varphi\colon L \to \Omega$ を定める．φ は K-線形写像である．φ がゼロ写像でないことを n に関する帰納法で証明する．

もし，$n = 1$ ならば，σ_1 は単射で $c_1 \neq 0$ だから，$\varphi = c_1\sigma_1$ はゼロ写像でない．

$n \geqq 2$ とする．φ がゼロ写像だと仮定して矛盾を導く．$\sigma_1(b) \neq \sigma_2(b)$ となる $b \in L$ がある．

$$0 = \varphi(bx) = \sum_{i=1}^{n} c_i\sigma_i(bx) = \sum_{i=1}^{n} c_i\sigma_i(b)\sigma_i(x)$$

なので，

$$0 = \sigma_1(b)\sum_{i=1}^{n} c_i\sigma_i(x) - \sum_{i=1}^{n} c_i\sigma_i(b)\sigma_i(x) = \sum_{i=2}^{n} \big(\sigma_1(b) - \sigma_i(b)\big)c_i\sigma_i(x)$$

となる．$c_i' := (\sigma_1(b) - \sigma_i(b))c_i$ とおくと，$\psi(x) := \sum_{i=2}^{n} c_i'\sigma_i(x)$ で定まる $\psi\colon L \to \Omega$ がゼロ写像になる．ここで，$c_2' \neq 0$ である．これは，帰納法の仮定に矛盾する． □

定理 9.6. K は体，L は K の巡回拡大体で $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ とする．$p := \mathrm{char}\, K$ は，$p = 0$ であるか $\mathrm{GCD}(p, n) = 1$ を満たすとする．また，K はすべての 1 の n 乗根を含むとする．このとき，ある元 $a \in L$ で $L = K(a)$ かつ a の K 上の最小多項式 $f_a(X)$ が $f_a(X) = X^n - b$ $(\exists b \in K)$ という形であるものが存在する．言い替えれば，$L = K(\sqrt[n]{b})$ と書ける．

証明. σ は巡回群 $\mathrm{Gal}(L/K)$ の生成元であるとする．$j \in \mathbb{Z}$ に対し σ^j が定義される．$\zeta \in K$ を 1 の原始 n 乗根とする．$\sigma \in \mathrm{Gal}(L/K)$ だから $\sigma(\zeta) = \zeta$ である．$x \in L$ に対して，

$$g(x) := \sum_{i=0}^{n-1} \zeta^i\sigma^i(x) \in L$$

とおく．ただし，$\sigma^0 = \mathrm{id}_L$ である．また，

$$\begin{aligned}\zeta\sigma(g(x)) &= \zeta\sigma\left(\sum_{i=0}^{n-2} \zeta^i\sigma^i(x)\right) + \zeta\sigma(\zeta^{n-1}\sigma^{n-1}(x)) = \sum_{i=0}^{n-2} \zeta^{i+1}\sigma^{i+1}(x) + \zeta^n\sigma^n(x)\\ &= \sum_{i=1}^{n-1} \zeta^i\sigma^i(x) + x = g(x) \qquad \text{①}\end{aligned}$$

となる．$\sigma_i = \sigma^{i-1}$, $c_i = \zeta^i$ として前補題を適用すると，$g(\omega) = \sum_{i=1}^{n} c_i\sigma_i(\omega) \neq 0$ を満たす $\omega \in L$ が存在する．$a := g(\omega) \in L$ とおく．① より $\sigma(\zeta a) = \sigma(\zeta g(\omega)) = g(\omega) = a$ なので，$\sigma(a) = \zeta^{-1}a$ である．$\sigma^i(a) = \zeta^{-i}a$ なので，a の K 上の共役元全体は $a, \zeta a, \zeta^2 a, \ldots, \zeta^{n-1}a$ である．$\varepsilon := \prod_{i=0}^{n-1} \zeta^i \in \{\pm 1\}$ である．$b := \prod_{i=0}^{n-1} \zeta^i a = \varepsilon a^n \in L$ とおけば，a の K 上の最小多項式は $X^n - b$ である．$[K(a) : K] = [L : K]$ なので $L = K(a)$ である． □

10. 円分多項式

可換整域 R において，0 でも可逆元でもない R の任意の元が有限個の素元の積に表せるとき，R は UFD(素元分解整域)であるといった．R が UFD とき $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ に対し，$a_0, \ldots, a_n$ で生成される R のイデアルを $\mathrm{cont}(f)$ と書くことにする．R が UDF で $\mathrm{cont}(f) = R$ のとき，f は**原始的** (primitive) であるという．

定理 10.1.(ガウスの補題) R は UFD，$f(X),\, g(X) \in R[X]$ とする．また，$K = Q(R)$ (分数体) とする．

(1) $f(X)$ と $g(X)$ が原始的ならば，$f(X)g(X)$ も原始的である．
(2) $f(X),\, g(X) \in R[X]$ で $g(X)$ は原始的であるとする．ある $h(X) \in K[X]$ が存在して $f(X) = g(X)h(X)$ と $K[X]$ 内で因数分解できるならば $h(X) \in R[X]$ である．
(3) $f(X) \in R[X]$ は原始的で $R[X]$ 内で既約ならば，$K[X]$ でも既約である．
(4) $f(X) \in R[X]$ はモニック多項式，$g(X),\, h(X) \in K[X]$ はモニック多項式で $f(X) = g(X)h(X)$ を満たすならば，$g(X),\, h(X) \in R[X]$ である．
(5) $f(X) \in R[X]$ がモニック多項式で，$\alpha \in K$ が $f(\alpha) = 0$ を満たせば $\alpha \in R$ である．

証明. (1) $\mathrm{cont}(fg) \neq R$ ならば，$\mathrm{cont}(fg) \subset pR$ となる R の素元 p が存在する．$f(X) = \sum_{i=0}^{n} a_i X^i$, $g(X) = \sum_{i=0}^{m} b_i X^i$ とする．$\mathrm{cont}(f) \notin pR$ だから，p の倍数でない a_i が存在する．そのような a_i の中で i が最小なものを a_k とする．$b_l \notin pR$ も同様に選ぶ．$f(X)g(X)$ の X^{k+l} の係数 c_{k+l} は，$c_{k+l} = \sum_{i+j=k+l} a_i b_j$ — ① によって得られる．$i < k$ のとき $a_i \in pR$, $j < l$ のとき $b_j \in pR$ だから，① の右辺に現れる $a_k b_l$ 以外の $a_i b_j$ は pR に属し，$a_k b_l \notin pR$ なので，$c_{k+l} \notin pR$ である．他方 $\mathrm{cont}(fg) \subset pR$ より $c_{k+l} \in pR$ であり，矛盾する．

(2) $h(X) = \sum_{i=0}^{l} \frac{c_i}{d_i} X^i$ ($c_i,\, d_i \in R$ で $(c_i,\, d_i) = R$) とし，$\alpha := \mathrm{LCM}(d_0, \ldots, d_l) \in R$ とする．すると，$\alpha h(X) \in R[X]$ である．また，$\beta R = \mathrm{cont}(\alpha h(X))$ を満たす $\beta \in R$ を取る．$h_0(X) := (\alpha/\beta)h(X) \in R[X]$ で，$h_0(X)$ は原始的である．$\gamma R = (\alpha,\, \beta)$ を満たす γ を取り，$\alpha = \gamma\alpha',\, \beta = \gamma\beta'$ ($\alpha',\, \beta' \in R$) と約分しておく．$\alpha' f(X) = \beta' g(X) h_0(X)$ である．もし，$\alpha' R \neq R$ ならば $\alpha' R \subset pR$ となる素元 p がある．β', $g(X)$, $h_0(X)$ は p の倍数であったが，β' は α' と互いに素で，$g(X)$ と $h_0(X)$ は原始多項式だから，p の倍数にはならない．よって，α' は R の可逆元で，$f(X) = g(X)((\beta'/\alpha')h_0(X)),\, ((\beta'/\alpha')h_0(X)) \in R[X]$ となる．

(2) $g(X),\, h(X) \in R[X]$ は $g(X)R[X] \neq R[X]$, $h(X)R[X] \neq R[X]$ を満たし，$f(X) = g(X)h(X)$ であるとする．

(3) $f(X) = g(X)h(X)$ ($g(X),\, h(X) \in K[X]$ は 1 次以上の多項式) とする．原始多項式 $g_0(X),\, h_0(X) \in R[X]$ と，$\mathrm{GCD}(a,\, b) = 1$ を満たす $a,\, b \in R$ により，$bf(X) = ag_0(X)h_0(X)$ と書ける．もし，$bR \neq R$ ならば $bR \subset pR$ となる素元 p を取ると，(2) の議論のように a, $\mathrm{cont}(g_0)$, $\mathrm{cont}(h_0)$ のいずれかは p の倍数になって矛盾する．よって，$1/b \in R$ で，$f(X)$ は $R[X]$ でも可約になる．

(4) (3) の証明のように，$bf(X) = ag_0(X)h_0(X)$ と表す．ここで，$g_0(X),\, h_0(X) \in R[X]$ は原始的，$a,\, b \in R$ で $\mathrm{GCD}(a,\, b) = 1$ とする．(3) と同じ議論で $1/b \in R$ が得られるから，$b = 1$ としてよい．すると，$f(X) = ag_0(X)h_0(X)$ の最高次の項を比較すれば，a も R の可逆元 ($a = 1$ としよう) で，$g_0(X)$, $h_0(X)$ もモニック多項式になる．

(5) $f(X) = (X - \alpha)g(X)$ ($\exists g(X) \in K[X]$) と書ける．(4) より，$X - \alpha,\, g(X) \in R[X]$ である． □

上の補題から $X^n - 1 \in \mathbb{Q}[X]$ の素因数分解は $\mathbb{Z}[X]$ の中で与えることができる．その既約因子について考察する．$\zeta_n = \exp(2\pi i/n)$ は $\mathbb{C}$ 内での 1 の原始 n 乗根とする．$k \in \mathbb{Z}$ に対して，その $n\mathbb{Z}$ を法とする同値類を $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ とするとき，$\zeta_n^n = 1$ だから，$\zeta_n^{\overline{k}} = \zeta_n^k$ と定義することができる．

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \overline{k} \;\middle|\; k \in \mathbb{Z},\, \mathrm{GCD}(k,\, n) = 1 \right\}$$

である．また，$\varphi(n)$ をオイラーのファイ関数とするとき，$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ であった以後，$\overline{k}$ は単に $k \in \mathbb{Z}/n\mathbb{Z}$ と書く．$\left\{ \zeta_n^k \;\middle|\; k \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}$ が $\mathbb{C}$ 内の 1 の原始 n 乗根全体の集合である．

定義 10.2.(円分多項式)

$$\Phi_n(X) := \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^k) \in \mathbb{C}[X]$$

とし，これを**円分多項式**という．

定理 10.3. $n \in \mathbb{N}$ とし，n の正の約数全体の集合を $D(n)$ とする．
(1) $\Phi_n(X) \in \mathbb{Z}[X]$ で，$\Phi_n(X)$ は $\mathbb{Q}[X]$ で既約である．
(2) $\displaystyle\prod_{d\in D(n)} \Phi_d(X) = X^n - 1$ である．

証明. (1) ζ_n の $\mathbb{Q}$ 上の共役元全体は $\{\zeta_n^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ なので，$\Phi_n(X)$ は $\mathbb{Q}$ 上の ζ_n の最小多項式である．よって，$\Phi_n(X) \in \mathbb{Q}[X]$ で，$\Phi_n(X)$ は $\mathbb{Q}[X]$ で既約である．$\Phi_n(X)$ は $X^n - 1 \in \mathbb{Z}[X]$ の約数でモニックなので，ガウスの補題より $\Phi_n(X) \in \mathbb{Z}[X]$ であって，$\mathbb{Z}[X]$ で既約である．

(2) $\mathbb{C}$ 内の 1 の原始 d 乗根全体の集合を $R(d)$ とおくと，

$$\bigcup_{d\in D(n)} R(d) = \{\zeta_n^k \mid 0 \leqq k < n\} = \{a \in \mathbb{C} \mid a^n = 1\}$$

である．また，$d_1 \neq d_2 \in D(n)$ のとき $R(d_1) \cap R(d_2) = \phi$ である．$\Phi_d(X)$ の根全体は $R(d)$ であるので，結論を得る． □

この定理の (2) を使って計算すると，

$$\begin{aligned}
&\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \quad (p \text{ は素数})\\
&\Phi_4(X) = X^2 + 1\\
&\Phi_6(X) = X^2 - X + 1\\
&\Phi_8(X) = X^4 + 1\\
&\Phi_9(X) = X^6 + X^3 + 1\\
&\Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1\\
&\Phi_{12}(X) = X^4 - X^2 + 1
\end{aligned}$$

となる．

定理 10.4. R は可換環，$S = R[X_1,\ldots, X_n]$ とし，$1 \leqq r \leqq n$ に対し，

$$s_r := \sum_{i_1<i_2<\cdots<i_r} X_{i_1}X_{i_2}\cdots X_{i_r}$$

とおく，s_r を $X_1,\ldots, X_n$ の r 次の**基本対称式**といった．

$$\prod_{i=1}^{n}(T - X_i) = T^n - s_1T^{n-1} + s_2T^{n-2} + \cdots + (-1)^{n-1}s_{n-1}T + (-1)^n s_n$$

である．いま，$f(X_1,\ldots, X_n) \in R[X_1,\ldots, X_n]$ が $X_1,\ldots, X_n$ の対称式ならば，ある $g(X_1,\ldots, X_n) \in R[X_1,\ldots, X_n]$ が存在して，

$$f(X_1,\ldots,X_n) = g(s_1,\ldots,s_n)$$

と書ける．

証明. 多項式の項を次数付き辞書式順序で順序付けして考える．つまり，$X_1^{i_1}\cdots X_n^{i_n}$ に対して，非負整数の組 $(i_1 + \cdots + i_n, i_1, i_2,\ldots, i_n)$ を辞書式順序で考えて項の次数の大小を比較する．

f の次数付き辞書式次数に関する超限帰納法で証明する．次数最小の対称式は定数多項式だから，この場合，定理は自明である．

f は定数多項式でない対称式とする．f に現れる次数付き辞書式順序で次数最大の項を $g = aX_1^{i_1}\cdots X_n^{i_n}$ とする．次数付き辞書式順序の定義から $i_1 \geqq i_2 \geqq \cdots \geqq i_n$ である．

$$h = s_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$$

とおく．h の次数最大の項は $X_1^{i_1}\cdots X_n^{i_n}$ なので，これは g の次数と一致している．よって，$f - ah$ の次数は f の次数より次数付き辞書式順序で真に小さい．帰納法の仮定より $f - ah$ は $s_1,\ldots, s_n$ の多項式で表せる． □

参考 10.5. R はネーター可換環とする．$f \in R[X_1,\ldots, X_n]$ に対し，

$$f = f(X_1,\ldots,X_n) = \sum_{i_1=0}^{d_1} \cdots \sum_{n_1=0}^{d_n} a_{i_1,\ldots,a_n} X_1^{i_1} \cdots X_n^{i_n} \quad (a_{i_1,\ldots,i_n} \in R)$$

に現れるすべての係数 $a_{i_1,\ldots,i_n}$ で生成される R のイデアルを $\mathrm{cont}(f)$ と書くことにする．すると，f, $g \in R[X_1,\ldots, X_n]$ に対し以下が成り立つ．

$$\mathrm{cont}(fg) \subset \mathrm{cont}(f)\,\mathrm{cont}(g) \subset \sqrt{\mathrm{cont}(fg)}$$

証明. f, g の項を辞書式順序で並べて，多重指数で $f(X) = \sum_i a_i X^i$, $g(X) = \sum_i b_i X^i$ と表わしておく．つまり $i = (i_1,\ldots, i_n)$ で $X^i = X_1^{i_1} \cdots X_n^{i_n}$.

(1) $\mathrm{cont}(fg) \subset \mathrm{cont}(f)\,\mathrm{cont}(g)$ を示す．f の係数全体を $\{a_i \mid i \in I\}$，g の係数全体を $\{b_j \mid j \in J\}$ とすると，fg の項の係数 c は何個かの $a_i b_j$ の和である．$a_i \in \mathrm{cont}(f)$, $b_j \in \mathrm{cont}(g)$ なので，$c \in \mathrm{cont}(f)\,\mathrm{cont}(g)$ である．よって $\mathrm{cont}(fg) \subset \mathrm{cont}(f)\,\mathrm{cont}(g)$ である．

(2) $\mathrm{cont}(f)\,\mathrm{cont}(g) \subset \sqrt{\mathrm{cont}(fg)}$ を示す．$\mathrm{cont}(fg) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ を準素イデアル分解とし，$\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ とする．$\mathrm{cont}(f)\,\mathrm{cont}(g) \not\subset \sqrt{\mathrm{cont}(fg)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ ならば，$\mathrm{cont}(f)\,\mathrm{cont}(g) \not\subset \mathfrak{p}_m$ となる m が存在する．$\mathfrak{p} := \mathfrak{p}_m$ は素イデアルだから，$\mathrm{cont}(f) \not\subset \mathfrak{p}$, $\mathrm{cont}(g) \not\subset \mathfrak{p}$ である．$a_i \notin \mathfrak{p}$, $b_j \notin \mathfrak{p}$ となる最小の $i = (i_1,\ldots, i_n)$, $j = (j_1,\ldots, j_n)$ を取る．$k = i + j = (i_1 + j_1,\ldots, i_n + j_n)$ とおくと，fg の X^k の係数 c_k は，$c_k = \sum_{i'+j'=k} a_{i'} b_{j'}$ —① によって得られる．$i' < i$ のとき $a_{i'} \in \mathfrak{p}$, $j' < j$ のとき $b_{j'} \in \mathfrak{p}$ だから，① の右辺に現れる $a_i b_j$ 以外の $a_{i'} b_{j'}$ は $\mathfrak{p}$ に属し，$a_i b_j \notin \mathfrak{p}$ なので，$c_k \notin \mathfrak{p}$ である．他方 $\mathrm{cont}(fg) \subset \mathfrak{p}$ より $c_{k+l} \in \mathfrak{p}$ であり，矛盾する． □

11. 方程式の可解性

定義 11.1. K は体，$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ とする．L は K 最小分解体とする．$f(a) = 0$ を満たす $a \in L$ が，$a_0,\ldots, a_{n-1}$ と四則 $+$, $-$, $\times$, $\div$ と根号 $\sqrt[k]{\ }$ (k はいろいろな自然数) と定まった整数 のみを用いた式で表せるとき，a は K 上**根号表示**できるという．$f(X)$ のすべての根が K 上根号表示できるとき $f(X) = 0$ は**代数的に解ける**とか，$f(X)$ は K 上**可解**であるという．

a が K 上根号表示できる，という定義を，拡大体の言葉で言い替えておく．$a_0,\ldots, a_{n-1} \in K$ のとき，$a_0,\ldots, a_{n-1}$ の有理式で表せる元は K に属するから，この段階では体の拡大は生じない．$b \in K$ に対し $\sqrt[k]{b}$ を取ると $K(\sqrt[k]{b})$ が $\sqrt[k]{b}$ と K を含む最小の体である．したがって，a が K 上**根号表示**できるための必要十分条件は，巡回拡大体の列 $K = K_0 \subset K_1 \subset \cdots \subset K_r \subset L$ で，任意の $1 \leqq i \leqq r$ に対してある $k_i \in \mathbb{N}$ と $b_i \in K_{i-1}$ が存在して $K_i = K_{i-1}(\sqrt[k_i]{b_i})$ となり，$a \in K_r$ となることである．この拡大体の列が $K_r = L$ を満たすようにとれることが，$f(X)$ が代数的に解けるための必要十分条件である．

拡大体の列 $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ で，任意の $1 \leqq i \leqq r$ に対して $K_i = K_{i-1}(\sqrt[k_i]{b_i})$ ($\exists k_i \in \mathbb{N}$, $\exists b_i \in K_{i-1}$) を満たすものが存在するとき，L は K の**巾根拡大**であるという．

定理 11.2. K は標数 0 の体で，ζ は 1 の n 乗根とする．
(1) ζ は K 上根号表示できる．
(2) $X^n - 1$ の最小分解体 L は K の巾根拡大である．

証明. (1) $\Phi_n(X)$ は円分多項式とし，M は $\mathbb{Q}$ 上の $\Phi_n(X)$ の最小分解体とする．M は $\mathbb{Q}$ 上 1 の原始 n 乗根で生成される巡回拡大で，$\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ で，$(\mathbb{Z}/n\mathbb{Z})^\times$ は巡回群の直和に書けるから M は $\mathbb{Q}$ の巾根拡大である．$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r = M$ で，$K_i = K_{i-1}(\sqrt[k_i]{b_i})$ となる列が存在する．$M_0 = K$, $M_i = M_{i-1}(\sqrt[k_i]{b_i})$ とおく．すると $K = M_0 \subset M_1 \subset \cdots \subset M_r = M$ となる．$M_i = M_{i-1}$ となる場合もあるが，それは気にしなくてよい．よって，ζ は根号表示できる．

(2) $\mathbb{Q}$ 上の $X^n - 1$ の最小分解体を M' とすると，(1) の結果から M' は $\mathbb{Q}$ の巾根拡大である．$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r = M' \subset L$ で，$K_i = K_{i-1}(\sqrt[k_i]{b_i})$ となる列が存在する．$L_0 = K$, $L_i = L_{i-1}(\sqrt[k_i]{b_i})$ とおく．すると $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ となる．よって，L は K の巾根拡大である． □

命題 11.3. K は標数 0 の体，$X^n - a \in K[X]$ は既約であると仮定する．また，ζ_n は 1 の原始 n 乗根とする．このとき，$\sqrt[n]{a}$ の $K(\zeta_n)$ 上の最小多項式は，$X^m - b$ ($\exists b \in K(\zeta)$ で m は n の約数) という形である．

証明. $\sqrt[n]{a}$ の K 上の共役が $\zeta_n^i \sqrt[n]{a}$ ($i \in (\mathbb{Z}/n\mathbb{Z})^\times$) という形であることからすぐわかる． □

定義 11.4. 一般に群 G (演算は積とする) に対し，$\left\{a^{-1}b^{-1}ab \;\middle|\; a, b \in G\right\}$ を含む G の最小の部分群を G の**交換子群**といい $[G, G]$ で表す．

$G_0 := G$, $G_{i+1} := [G_i, G_i]$ ($i \geqq 0$) で $G_0 \supset G_1 \supset \cdots$ を定義するとき，ある $r \in \mathbb{N}$ が存在して $G_r = \{1\}$ となるばらば，G は**可解群**であるという．$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ を G の**可解列**という．

命題 11.5. G は群とする．

(1) $[G, G] \lhd G$ である．

(2) $G/[G, G]$ はアーベル群である．

(3) 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ で，各 $i = 1,\ldots, r$ に対して G_{i-1}/G_i がアーベル群になるものが存在すれば，G は可解群である．

(4) $N \lhd G$ で，G/N と N が可解群ならば，G も可解群である．

(5) G が有限可解群ならば，正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ で，各 $i = 1,\ldots, r$ に対して G_{i-1}/G_i が巡回群になるものが存在する．

証明. $a, b \in G$ に対し，$[a, b] := a^{-1}b^{-1}ab$ と書く．

(1) $a, b, c \in G$ のとき，$a' = c^{-1}ac$, $b' = c^{-1}bc$ とおくと，$c^{-1}[a, b]c = [a', b']$ だから．

(2) $ba = abb^{-1}a^{-1}ba = ab[b, a] \in ab[G, G]$ である．よって，$ba[G, G] = ab[G, G]$ で，$G/[G, G]$ はアーベル群である．

(3) $\pi_i : G_{i-1} \longrightarrow G_{i-1}/G_i$ を自然な全射とする．$\pi_i([G_{i-1}, G_{i-1}]) \neq \{1\}$ とすると，ある $a, b \in G_{i-1}$ で $[a, b] \notin G_i$ となるものが存在する．つまり，$\pi_i(a^{-1}b^{-1}ab) \neq 1$ なので，$\pi_i(a)\pi_i(b) \neq \pi_i(b)\pi_i(a)$ となる．これは G_{i-1}/G_i がアーベル群であることに矛盾する．よって，$[G_{i-1}, G_{i-1}] \lhd G_i$ である．

$N_0 := G$, $N_i := [N_{i-1}, N_{i-1}]$ ($i \geqq 1$) で正規列 $G = N_0 \rhd N_1 \rhd \cdots$ を定める．$N_{i-1} \subset G_{i-1}$ ならば，$N_i = [N_{i-1}, N_{i-1}] \subset [G_{i-1}, G_{i-1}] = G_i$ なので，i に関する帰納法で，$N_i \subset G_i$ が証明できる．よって，$N_r = \{1\}$ で，G は可解群である．

(4) $\pi : G \to G/N$ を自然な全射とする．$H_0 := G/N$, $H_{i+1} = [H_i, H_i]$ ($i \geqq 0$) とするとき，ある $m \in \mathbb{N}$ で $H_m = \{1\}$ となる．$N_i := \pi^{-1}(H_i)$ とおくと，$G = N_0 \rhd N_1 \rhd \cdots \rhd N_m = N$ で，各 $i = 1,\ldots, m$ に対して N_{i-1}/N_i がアーベル群になる．これに N の可解列をつなげば，(3) を満たす G の正規列が得られる．

(5) 有限アーベル群の構造定理からわかる． □

定理 11.6. K は標数 0 の体，L は K の有限次ガロア拡大体とする．L が K の巾根拡大であるための必要十分条件は，$\mathrm{Gal}(L/K)$ が可解群であることである．

証明. (1) $G := \mathrm{Gal}(L/K)$ が可解群ならば L は K の巾根拡大であることを示す．

$G_0 := G$, $G_{i+1} := [G_i, G_i]$ とし，$G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ と仮定する．r に関する帰納法で証明する．

(1-1) $r = 1$ の場合．

$G/[G, G]$ はアーベル群で，$[G, G] = \{1\}$ なので，G はアーベル群である．有限アーベル群の構造定理より，G の (正規) 部分群の列 $G = H_0 \rhd H_1 \rhd \cdots \rhd G_m = \{1\}$ で，H_{i-1}/H_i ($1 \leqq \forall \leqq m$) が巡回群であるようなものが存在する．$M_i := M^{H_i}$ とおくと，定理 9.6 より，$M_i = M_{i-1}(\sqrt[n_i]{b_i})$ ($\exists n_i \in \mathbb{N}$, $\exists b_i \in M_{i-1}$) と書ける．$M_0 = L$, $M_m = L$ なので，L は K の巾根拡大である．

(1-2) $r \geqq 2$ の場合．

$L_i = L^{G_i}$ とおく．$r = 1$ の場合の結果から，L_i は L_{i-1} の巾根拡大である．よって，L は K の巾根拡大である．

(2-1) $L = K(\sqrt[n]{a})$ ($a \in K$) ならば，$G := \mathrm{Gal}(L/K)$ が可解群であることを証明する．

ζ_n を 1 の原始 n 乗根とすると，$\sqrt[v]{a}$ の K 上の共役は $\zeta_n^i \sqrt[v]{a}$ という形なので，L/K がガロア拡大ならば $\zeta_n^i \sqrt[v]{a} \in L$ である．$K(\zeta_n)$ は K のアーベル拡大なので，$H_1 := \mathrm{Gal}(K(\zeta_n)/K)$ はアーベル群であり，$[H_1, H_1] = \{1\}$ だから可解群である．

$\sqrt[v]{a}$ の $K(\zeta_n)$ 上の最小多項式は，$X^m - b$ $(\exists b \in K(\zeta))$ という形であったので，$L = K(\zeta_n)(\sqrt[m]{b})$ である．よって，$H_2 := \mathrm{Gal}(L/K(\zeta_n)) \cong \mathbb{Z}/m\mathbb{Z}$ である．H_2 は G の正規部分群で，$G/H_2 \cong H_1$ である．前命題より，G は可解群である．

(2-2) L が K の巾根拡大ならば，$G := \mathrm{Gal}(L/K)$ が可解群であることを，$[L : K]$ に関する帰納法で証明する．$[L : K] = 2$ の場合は (2-1) からわかる．

$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$, $K_i = K_{i-1}(\sqrt[k_i]{b_i})$ となる巡回拡大の列がある．$n = k_1$, $b = b_1 \in K$ とおくと，$K_1 = K(\sqrt[n]{b})$ である．$\sqrt[n]{b}$ の K 上の共役は $\zeta_n^i \sqrt[n]{a}$ という形なので，$M := K_1(\zeta_n)$ は K のガロア拡大で，巾根拡大である．$M = L$ ならば，(2-1) の場合に帰着される．そこで，$M \subsetneqq L$ の場合を考える．帰納法の仮定から，$H := \mathrm{Gal}(M/K)$ は可解群である．

$M_i = M_{i-1}(\sqrt[k_i]{b_i})$ とおくと，$M = M_1 \subset K_2 \subset \cdots \subset M_r = L$ なので，L は M のガロア拡大で巾根拡大である．よって，帰納法の仮定から $N := \mathrm{Gal}(G/M)$ も可解群である．また，N は G の正規部分群で，$G/N \cong H$ である．前命題から，G は可解群である． □

12．5 次以上の方程式

まず，可解群についてのいくつかの定理を述べておく．

定理 12.1. *G が可解群ならば，G の部分群 H も可解群である．*

証明. $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ を G の可解列とする．$H_i := H \cap G_i$ とおく．各 $1 \leqq i \leqq r$ に対して．$G_i \lhd G_{i-1}$ より $H_i \lhd H_{i-1}$ である．同型定理より，

$$H_{i-1}/H_i = H_{i-1}/(G_i \cap H_{i-1}) \cong H_{i-1}G_i/G_i \subset G_{i-1}/G_i$$

で，G_{i-1}/G_i がアーベル群なので H_{i-1}/H_i もアーベル群である．よって，H も可解群である． □

自然数 n に対し $X_n := \{1, 2, \ldots, n\}$ とし，

$$\mathfrak{S}_n := \{\sigma \mid \sigma : X \to X \text{ は全単射}\}$$
$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \mathrm{sign}(\sigma) = 1\}$$

とおく．ここで，$\mathrm{sign}(\sigma)$ は置換 σ の符号である．$\mathfrak{S}_n$ を n 次**対称群**, $\mathfrak{A}_n$ を n 次**交代群**といった．

定理 12.2.
(1) $n \leqq 4$ のとき，$\mathfrak{S}_n$, $\mathfrak{A}_n$ は可解群である．
(2) $n \geqq 5$ のとき，$\mathfrak{S}_n$, $\mathfrak{A}_n$ は可解群でない．

証明. (1) $n \leqq 4$ のとき $\mathfrak{S}_n$ と $\mathfrak{A}_n$ は $\mathfrak{S}_4$ の部分群であるので，$\mathfrak{S}_4$ が可解群であることを示せばよい．
$1 \leqq i < j \leqq 4$ に対して $(i, j) \in \mathfrak{S}_4$ は i と j の互換を表すとし，

$$V_4 := \{\mathrm{id}_{X_4}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

とすると，$\mathfrak{S}_4 \rhd \mathfrak{A}_4 \rhd V_4 \rhd \{1\}$ で，$\mathfrak{S}_4/\mathfrak{A}_4 \cong \mathbb{Z}/2\mathbb{Z}$, $\mathfrak{A}_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, $V_4/\{1\} = V_4 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ である．よって，$\mathfrak{S}_4$ は可解群である．

(2) $n \geqq 5$ のとき $\mathfrak{S}_n$ と $\mathfrak{A}_n$ は $\mathfrak{A}_5$ を部分群として含むので，$\mathfrak{A}_5$ が可解群でないことを示せばよい．
$(i, j) = (1, i)(1, j)(1, i) \in \mathfrak{S}_5$ で，$\mathfrak{A}_5$ の元は偶数個の互換の積で表せるから，$\mathfrak{A}_5$ の元は $(1, i)$ $(2 \leqq i \leqq 5)$ という形の互換偶数個の積で表せる．
$1 \leqq i < j < k \leqq 5$ に対し，$(i, j, k) \in \mathfrak{A}_5$ は i, j, k の巡回置換 $(i \to j, j \to k, k \to i.$ これは偶置換である) を表すとする．$(1, 2)(1, j) = (1, 2, j)^2$, $(1, i)(1, j) = (1, 2, i)(1, 2, j)^2$ だから，$\mathfrak{A}_5$ は $(1, 2, 3)$ と $(1, 2, 4)$ と $(1, 2, 5)$ で生成される．
今，i, j, k は 3, 4, 5 の置換であるとする．巡回置換は偶置換だから，$\sigma := (k, i, i) \in \mathfrak{A}_5$, $\tau := (j, 2, k) \in \mathfrak{A}_5$ である．ところが，

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau = (1,i,k)(k,2,j)(k,i,1)(j,2,k) = (1,2,k)$$

である．したがって，$[\mathfrak{A}_5, \mathfrak{A}_5] = \mathfrak{A}_5$ である．よって，$\mathfrak{A}_5$ は可解群でない． □

定理 12.3.
$\omega_1,\ldots,\omega_n \in \mathbb{C}$ は $\mathbb{Q}$ 上 1 次独立とし，$\omega_1,\ldots,\omega_n$ の k 次の基本対称式を $c_k \in \mathbb{C}$ とする．$K := \mathbb{Q}(c_1,\ldots,c_n)$, $L := \mathbb{Q}(\omega_1,\ldots,\omega_n)$ とおく．すると，L は K のガロア拡大で，$\mathrm{Gal}(L/K) \cong \mathfrak{S}_n$ である．

証明. $\sigma \in \mathfrak{S}_n$ に対して $\sigma(\omega_i) = \omega_{\sigma(i)}$ で，$a \in \mathbb{Q}$ に対しては $\sigma(a) = a$ と定めて $\mathfrak{S}_n$ を L に作用される．σ は $\omega_1,\ldots,\omega_n$ の置換とみなせ，$\mathrm{Aut}(L/K)$ の元とみなせる．$M := L^{\mathfrak{S}_n}$ とおく．M の元は f/g (f, $g \in L$) と表せる．$h := \prod_{\sigma\in\mathfrak{S}_n-\{id\}} \sigma(g)$ とおくと $\sigma(gh) = gh$ である．$\sigma(f/g) = f/g$ より $\sigma(fh) = fh$ である．よって，$M = Q\big(\mathbb{Q}[\omega_1,\ldots,\omega_n]^{\mathfrak{S}_n}\big)$ である．他方，対称式は基本対称式の多項式で表せるから，$\mathbb{Q}[\omega_1,\ldots,\omega_n]^{\mathfrak{S}_n} = \mathbb{Q}[c_1,\ldots,c_n]$ である．よって，$M = Q\big(\mathbb{Q}[c_1,\ldots,c_n]\big) = K$ である．$L^{\mathfrak{S}_n} = K$ だから，定理 8.3 より，L は K のガロア拡大で，$\mathfrak{S}_n = \mathrm{Gal}(L/K)$ が成り立つ． □

標数 0 の体で考えるとき，上の定理は，5 次以上の方程式については，(根号と四則のみを用いた) 解の公式が存在しないことを意味する．$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_n$ ($n \geqq 5$) の解の公式があるということは，$f(X) = 0$ の解 $\omega_1,\ldots,\omega_n$ を $a_1,\ldots,a_n$ の四則と根号を用いた式で表せる，ということで，言い換えると $L := \mathbb{Q}(\omega_1,\ldots,\omega_n)$ が $K := \mathbb{Q}(a_1,\ldots,a_n)$ の巾根拡大である，ということである．しかし，$\mathrm{Gal}(L/K) \cong \mathfrak{S}_n$ で，$n \geqq 5$ のとき，これは可解群でないので，L は K の巾根拡大ではない．したがって，上に述べた意味での解の公式は存在しない．

考察 12.4.(3 次方程式) 定理 12.3 において $n = 3$ とする．$\mathrm{Gal}(L/K) = \mathfrak{S}_3 \rhd \mathfrak{A}_3 \rhd \{1\}$ は，$\mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbb{Z}/2Z$, $\mathfrak{A}_3/\{1\} = \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ を満たし，$\mathrm{Gal}(L/K) = \mathfrak{S}_3$ は可解群である．$M = L^{\mathfrak{A}_3}$ とおくと，$\mathrm{Gal}(L/M) = \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ であるので，ある $b_2 \in M$ が存在して $L = M(\sqrt[3]{b_2})$ と書ける．$\omega = \zeta_3$ を 1 の原始 3 乗根とするとき，$\omega\sqrt[3]{b_2}$ は $\sqrt[3]{b_2}$ の共役元なので，$\omega \in L$ でなければならない．また，$\mathrm{Gal}(M/K) = \mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbb{Z}/2\mathbb{Z}$ であるので，ある $b_1 \in M$ が存在して $M = K(\sqrt{b_1})$ と書ける．実際，3 次方程式の解の公式には平方根と立方根が現れる．

考察 12.5.(4 次方程式) 定理 12.3 において $n = 4$ とする．$\mathfrak{S}_4 \rhd \mathfrak{A}_4 \rhd V_4 \rhd \mathbb{Z}/2\mathbb{Z} \rhd \{1\}$ で，$\mathfrak{S}_4/\mathfrak{A}_4 \cong \mathbb{Z}/2\mathbb{Z}$, $\mathfrak{A}_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, $V_4 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ であった．上と同じ考察で，この列に対応して，

$$K \subset M_1 := K(\sqrt{b_1}) \subset M_2 := M_1(\sqrt{b_2}) \subset M_3 := M_3(\sqrt[3]{b_3}) \subset M_3(\sqrt{b_4}) = L$$

($b_1 \in K$; $b_{i+1} \in M_i$ $(i = 1, 2, 3)$) という巾根拡大の列が存在する．よって，4 次方程式の公式には，3 次方程式を解く操作が必要になる．

13. 正多角形の作図

本章では，正 n 角形が目盛りのない直線定規とコンパスのみを用いて作図可能であるための必要十分条件を考察する．まず「目盛りのない直線定規とコンパスのみを用いて作図可能」というフレーズを，数学的に解釈しておく必要がある．

今，平面上に 1 つの円と，その円の中心を通る直交する 2 直線が描かれているとする (そういう作図は可能である)．このとき，円の中心を $(0, 0)$, 円と直線の 4 個の交点が $(\pm1, 0)$, $(0, \pm1)$ となるように平面に座標を設定して，この平面を座標平面 $\mathbb{R}^2$ と考える．さらに，$(1, 0)$ を $1 \in \mathbb{C}$, $(0, 1)$ を虚数単位 $\sqrt{-1} \in \mathbb{C}$ と同一視し，この平面は複素数平面 (ガウス平面) $\mathbb{C}$ であると考える．多角形の平行移動と相似拡大は，定規とコンパスのみで可能であるので，原点を中心とする半径 1 の円に内接する正 n 角形が作図可能か否か，という問題と同値になる．正 n 角形の 1 つの頂点を P_0 とし，そこから半時計回りに $P_1,\ldots,P_{n-1}$ と頂点に記号を付ける．P_0 は単位円周上にあらかじめ与えられていると仮定してよい．最初に座標軸を描く段階で，$P_0 = 1$ ($\mathbb{R}^2$ で言えば $(1, 0)$) となるように設定しておくことができる．そうすると，正 n 角形が作図可能であることと，1 の原始 n 乗根 ζ_n が作図可能であることは同値になる．

任意の整数 $k \in \mathbb{Z}$ に対し，0, $1 \in \mathbb{C}$ を結ぶ線分をもとにして，複素数平面に k や $k\sqrt{-1}$ に対応する点を作図することは可能である．また，$r \in \mathbb{N}$ に対して，線分の r 等分点も作図可能であるから，a, $b \in \mathbb{Q}$ に対して $a + b\sqrt{-1}$ に対応する点も作図可能である．一般に，z_1, $z_2 \in \mathbb{C}$ に対応する点が作図さ

れていれば，$z_1 \pm z_2$, $z_1 z_2$, z_1/z_2 ($z_2 \neq 0$ の場合) に対応する点も作図可能である．したがって，ζ_n が作図可能ならば $\mathbb{Q}(\zeta_n)$ に属する任意の点も作図可能である．

今，$\mathbb{C}$ 上に何個かの点 $z_1,\ldots, z_m \in \mathbb{C}$ が作図されているとし，$K_m := \mathbb{Q}(z_1,\ldots, z_m)$ とおく．z_1 と z_2 を結ぶ直線 ℓ_1 と，z_3 と z_4 を結ぶ直線 ℓ_2 の交点に対応する複素数を z_{m+1} とすると，z_{m+1} は $z_1,\ldots, z_4$ の有理式で表せるので，$z_{m+1} \in K_m$ である．つまり $K_{m+1} = K_m(z_{m+1})$ とおいても $K_{m+1} = K_m$ である．

直線 ℓ と円 C の交点を作図した場合を考える．ℓ_1 は z_1 と z_2 を結ぶ直線，r は z_3 と z_4 を両端とする線分の長さ，$q \in \mathbb{Q}$ は正の有理数とし，円 C は z_5 を中心とする半径 qr の円か，または，z_5, z_6, z_7 の 3 点を通る円とする．円の作図として許されているのは本質的にはこの 2 通りしかない．

ℓ と C の 2 交点を z_{m+1}, z_{m+2} とおくとき，その計算は 2 次方程式の根の計算に帰着されるから，ある $a_m \in K_m$ が存在し，z_{m+1}, $z_{m+2} \in K_m(\sqrt{a_m})$ となる．z_{m+1}, z_{m+2} が 2 円の交点の場合も同様である．

逆に $a \in \mathbb{C}$ が与えられてとき $\sqrt{a}$ を作図する方法はよく知られている．つまり，$\mathbb{R}^2$ のほうで考えて，点 $(0, 1/2)$ を中心に半径 $a + 1/2$ の円を描き，この円と直線 $y = a$ の交点の 1 つを P とすると $P = (\sqrt{a}, a)$ となる．

したがって，$w \in \mathbb{C}$ が目盛りのない直線定規とコンパスのみを用いて作図可能な点であるとは，ある $m \in \mathbb{N}$ と拡大体の列 $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$ が存在して，各 $1 \leqq i \leqq m$ に対してある $a_i \in K_{i-1}$ が存在して $K_i = K_{i-1}(\sqrt{a_i})$ であり，$w \in K_m$ となることである．以上より，次の定義が正当化される．

定義 13.1. ある $m \in \mathbb{N}$ と拡大体の列 $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$ — ① が存在して，各 $1 \leqq i \leqq m$ に対してある $a_i \in K_{i-1}$ が存在して $K_i = K_{i-1}(\sqrt{a_i})$ となるとき，拡大体の列 ① を $\mathbb{Q}$ の **2 次拡大の列**と呼ぶことにする．また，$\zeta_n \in \mathbb{C}$ は 1 の原始 n 乗根とする．正 n 角形が (定規とコンパスによって) **作図可能**であるとは，ある $\mathbb{Q}$ の 2 次拡大の列 ① が存在して $\zeta_n \in K_m$ となることをいう．

補題 13.2. $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$, $K_i = K_{i-1}(\sqrt{a_i})$ ($a_i \in K_{i-1}$, $1 \leqq i \leqq m$) を 2 次拡大の列とする．

(1) 必要なら，$i = m+1, m+2,\ldots$ に対して，ある $a_i \in K_{i-1}$ を選んで $K_i = K_{i-1}(\sqrt{a_i})$ を作る操作をうまく行えば，ある $n \geqq m$ が存在して K_n は $\mathbb{Q}$ のガロア拡大になるようにできる．

(2) $a \in K_m$ の $\mathbb{Q}$ 上の最小多項式を $f_a(X)$ とする．すると，ある $r \in \mathbb{N} \cup \{0\}$ が存在し，$\deg f_a(X) = 2^r$ となる．

証明. (1) $L = K_m$, $b_i = \sqrt{a_i}$ とおくと，$L = K_m = \mathbb{Q}(b_1,\ldots, b_m)$ である．今，b_i の $\mathbb{Q}$ 上のある共役元 b_i' が $b_i' \notin L$ であるとする．$\sigma(b_i) = b_i'$ となる $\sigma \in \mathrm{Mon}_{\mathbb{Q}}(K_m, \mathbb{C})$ を取る．$L_0 := L$, $L_j := L_{j-1}(\sigma(b_j)) = L_{j-1}(\sqrt{\sigma(a_j)})$ ($1 \leqq j \leqq i$) とおけば，$b_i' \in L_i$ である．

$\mathbb{Q}$ に $b_1,\ldots, b_m$ のすべての $\mathbb{Q}$ 上の共役元を付け加えて得られる体を F とする．定理 8.2 より，F は $\mathbb{Q}$ の有限次ガロア拡大である．上の考察から L から F に到達する 2 次拡大の列が存在する．

(2) (1) の結果から K_m は $\mathbb{Q}$ のガロア拡大であると仮定してよい．$f_a(X)$ の $\mathbb{Q}$ 上の最小分解体を M とする．$\mathrm{Gal}(L/M)$ は $\mathrm{Gal}(L/\mathbb{Q})$ の部分群で，$\#\mathrm{Gal}(L/\mathbb{Q}) = 2^l$ ($\exists l \in \mathbb{N} \cup \{0\}$) と書けるから，$\#\mathrm{Gal}(L/M) = 2^s$ ($0 \leqq s \leqq l$) と書ける．すると $\deg f_a(X) = [M : \mathbb{Q}] = [L : \mathbb{Q}]/[L : M] = 2^{l-s}$ である．□

フェルマー素数は $p^{2^r} + 1$ という形の素数のことで，以下の定理に出てくる素数と混同しないこと．

定理 13.3. p は 3 以上の素数とする．正 p 角形が作図可能であるための必要十分条件は，ある $r \in \mathbb{N}$ が存在して $p = 2^r + 1$ と書けることである．

証明. (必要性) 1 の原始 p 乗根 ζ_p の最小多項式は円分多項式

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

であった．補題 13.2(2) より，$p - 1 = \deg \Phi_p(X) = 2^r$ でないといけない．

(十分性) $L = \mathbb{Q}[\zeta_p]$ とおくと，上の考察から $[L : \mathbb{Q}] = 2^r$ である．また，定理 9.4 より L は $\mathbb{Q}$ のアーベル拡大である．有限アーベル群の構造定理により，$\mathrm{Gal}(L/\mathbb{Q}) = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$, $G_{i-1}/G_i \cong \mathbb{Z}/2\mathbb{Z}$ ($1 \leqq \forall i \leqq r$) を満たす $\mathrm{Gal}(L/\mathbb{Q})$ の部分群の列が存在する．$M_i := L^{G_i}$ とおくと，$M_r = L$, $M_0 = \mathbb{Q}$ で，$[M_i : M_{i-1}] = 2$ だから，ある $a_i \in M_{i-1}$ により $M_i = M_{i-1}(\sqrt{a_i})$ と書ける．

M_{i-1} の各点が作図可能ならば $\sqrt{a_i}$ も作図可能で，M_i の各点も作図可能である．よって，ζ_p も作図可能である． □

定理 13.4. n は 3 以上の整数とする．正 n 角形が作図可能であるための必要十分条件は，ある s, $m \in \mathbb{N} \cup \{0\}$ と相異なる素数 $p_1,\ldots,\ p_m$ で，$p_i = 2^{r_i} + 1$ $(\exists r_i \in \mathbb{N})$ という形のものが存在して $n = 2^s p_1 p_2 \cdots p_m$ と書けることである．

証明. (十分性) 一般に，l, m が互いに素な自然数で，$\mathbb{C}$ の原点を中心とする単位円に内接する正 k 角形と正 l 角形でひとつの頂点を共有するものが描かれていたら，2 つの多角形の頂点をうまく選んで中心角が $2\pi/kl$ になるようにできる．よって，正 kl 角形も作図可能である．このことから，m に関する帰納法で，正 $2^s p_1 p_2 \cdots p_m$ 角形も作図可能であることがわかる．

(必要性) 今，正 n 角形が作図可能であると仮定する．$n = 2^s p_1^{e_1} p_2^{e_2} \cdots p_m^{e_n}$ ($p_1,\ldots, p_m$ は相異なる奇素数) と因数分解する．正 n 角形が作図可能ならば，正 p_i 角形も作図可能だから，$p_i = 2^{r_i} + 1$ $(\exists r_i \in \mathbb{N})$ でないといけない．あと，$e_1 = \cdots = e_m = 1$ であることを示せばよい．

それには，p が奇素数のとき，正 p^2 角形は作図不可能であることを示せばよい．$p = 2^r + 1$ $(\exists r \in \mathbb{N})$ であった．$\varphi(n)$ をオイラーのファイ関数とするとき，$[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}] = \varphi(p^2) = p(p-1) = 2^r p$ である．補題 13.2(2) より ζ_{p^2} は作図不可能である． □

14. 複素数体

複素数体 $\mathbb{C}$ が代数閉体であることの証明はいろいろ知られていて，複素関数論の最大値の原理を使った証明が一番簡単だと思う．しかし，以下のようなガロア理論を用いた証明も可能である．ただ，中間値の定理から導かれる以下の 2 つの解析学系の定理が必要である．ペアノの公理から始めて $\mathbb{R}$ を定義する段階で，コーシー有理数列の極限として実数を定義するが，それを用いて中間値の定理も証明される．$\mathbb{R}$ の性質の証明に，多少の解析学が必要なのは仕方がない．

定理 14.1. $f(x) \in \mathbb{R}[x]$ が奇数次の多項式ならば，$f(a) = 0$ を満たす $a \in \mathbb{R}$ が存在する．

証明. $f(x)$ はモニック多項式と仮定してよい．すると，$x \gg 0$ のとき $f(x) > 0$ であり，$x \ll 0$ のとき $f(x) < 0$ である．よって，中間値の定理から $f(a) = 0$ を満たす $a \in \mathbb{R}$ が存在する． □

定理 14.2. $a \in \mathbb{R}$, $a > 0$ ならば $b^2 = a$ を満たす $b \in \mathbb{R}$, $b > 0$ が存在する．

証明. $f(x) = x^2 - a$ とおくとき，$x \gg 0$ のとき $f(x) > 0$ で，$f(x) = -a < 0$ なので，中間値の定理より，$b^2 - a = f(b) = 0$ となる $b \in \mathbb{R}$, $b > 0$ が存在する． □

群論から，次の定理を使う．

定理 14.3. G は有限群で $\#G = 2^n$ $(n \in \mathbb{N})$ であるとする．すると，G の部分群 H で $\#H = 2^{n-1}$ を満たすものが存在する．

証明. G の演算は積で表すことにする．

n に関する帰納法で証明する．$n = 1$ のときは，$H = \{1\}$ とおけばよい．

$n \geqq 2$ の場合を考える．

$$Z(G) := \left\{ a \in G \;\middle|\; \text{任意の } x \in G \text{ に対し } ax = xa \right\}$$

を G の中心といった．群論でよく知られているように，$Z(G)$ は G の正規部分群である．また，類等式に関する次の定理があった．$x \in G$ に対し，

$$Cx := \left\{ axa^{-1} \in G \;\middle|\; a \in G \right\}$$

と書くことにする．このとき，以下が成り立つ．

(1) 有限個の $x_1, x_2,\ldots, x_r \in G$ が存在して，

$$G = Cx_1 \sqcup Cx_2 \sqcup \cdots \sqcup Cx_r$$

が成り立つ．

(2) $\#G = \#Z(G) + \sum_{\#Cx_i \geqq 2} \#Cx_i$ が成り立つ．

(2) が類等式である．ところで，$Z_x := \{a \in G \mid ax = xa\}$ とおくと，Z_x は G の部分群である．

(3) $\#Cx = \#(G/Z_x)$ を示す．

$f: G \to C_x$ を $f(a) = axa^{-1} \in Cx$ $(a \in G)$ で定めるとき，「$f(a) = f(b) \iff axa^{-1} = bxb^{-1} \iff x = (a^{-1}b)xb^{-1}a = (a^{-1}b)x(a^{-1}b)^{-1} \iff (a^{-1}b)x = x(a^{-1}b) \iff a^{-1}b \in Z_x$」である．よって，$f$ から全単射 $\overline{f}: G/Z_x \longrightarrow Cx$ が導かれる．

(4) Z_x は G の部分群なので $\#Z_x$ は $\#G = 2^n$ の約数である．よって，$\#Cx$ も 2^n の約数である．特に，$\#Cx \geqq 2$ ならば $\#Cx$ は偶数である．類等式 (2) より，$\#Z(G)$ は偶数である．特に，$Z(G) \neq \{1\}$ である．

(5) もし $Z(G) = G$ ならば，G はアーベル群だから，有限アーベル群の構造定理により，G は $\mathbb{Z}/2^k\mathbb{Z}$ という形の巡回群の直和であり，この場合，定理は簡単に証明できる．

(6) $Z(G) \neq G$ の場合を考える．$\#G/Z(G) < \#G$ で $\#G/Z(G) = 2^k$ $(1 \leqq k < n)$ だから，帰納法の仮定により，ある部分群 $H' \subset G/Z(G)$ で $\#H' = 2^{k-1}$ を満たすものが存在する．$\pi: G \to G/Z(G)$ を自然な単射として $H := \pi^{-1}(H')$ とおけば，$G/H \cong (G/Z(G))/H' \cong \mathbb{Z}/2\mathbb{Z}$ だから $\#H = 2^{n-1}$ となる． □

定理 14.4. $\mathbb{C} = \mathbb{R}(\sqrt{-1}\,)$ は代数閉体である．

証明. (i) $C := \mathbb{R}(\sqrt{-1}\,)$ とする．$a \in C$ ならば $\sqrt{a} \in C$ であることを証明する．(最初から C を $\mathbb{C}$ と書いてしまうと，うっかり $\mathbb{C}$ の性質を使ってしまいそうになる.)

$a = b + c\sqrt{-1}$ $(a, b \in \mathbb{R})$ とする．

$$\left(\sqrt{\frac{\sqrt{b^2+c^2}+b}{2}} + \sqrt{-1}\sqrt{\frac{\sqrt{b^2+c^2}-b}{2}}\right)^2 = b + c\sqrt{-1}$$

なので，$\sqrt{a} \in C$ である．

(ii) $\overline{\mathbb{R}}$ を C の代数閉包とする．$\omega \notin \mathbb{R}(\sqrt{-1}\,)$ となる $\omega \in \overline{\mathbb{R}}$ が存在したと仮定して矛盾を導く．

C を含む $\mathbb{R}$ の有限次ガロア拡大 L を取る．ガロア群を $G := \mathrm{Gal}(L/\mathbb{R})$ とし，G の 2-シロー群 S を取る．

$$M := \{a \in L \mid \text{任意の } \sigma \in S \text{ に対し } \sigma(a) = a\}$$

とすると，M の $\mathbb{R}$ 上の拡大次数は $[M : \mathbb{R}] = \#G/\#S$ で，これは奇数である．勝手な $\alpha \in M$ の $\mathbb{R}$ 上の最小多項式 $f_\alpha(x)$ は奇数次であるが．定理 14.1 より $f_\alpha(x)$ は 1 次式であり，$M = \mathbb{R}$ となる．よって，$G = S$ で $\#G = 2^n$ と書ける．$n \geqq 2$ と仮定して矛盾を導こう．

$$H = \{\sigma \in G \mid \text{任意の } a \in C \text{ に対し } \sigma(a) = a\}$$

とおく．$\#(G/H) = 2$ だから $\#H = 2^{n-1}$ である．前定理から，H の部分群 I で $\#I = 2^{n-2}$ を満たすものが存在する．I に対応する C の 2 次拡大 $C(\sqrt{\alpha})$ $(\exists \alpha \in C)$ が存在する．しかし，(ii) の結果から $\sqrt{\alpha} \in C$ で，これは矛盾である．よって，$n = 1$ で $C = \overline{\mathbb{R}}$ である． □