代数学 III　授業ノート

Ziphil Aleshlas

2017 年 1 月 10 日

目次

1. 初めに

このノートは，2016 年度 A セメスターに東京大学理学部数学科で開講されている『代数学 III』の授業ノートです．内容としては，体と Galois 理論を扱います．執筆者の気分によって，講義で扱われた内容でもここに書いていなかったり，講義で触れられていない内容が書かれていたりしますが，概ね講義の内容そのままになっています．

実際に講義中で使われた記号や言葉が個人的に気に入らないなどの理由で，勝手に記号や言葉を変えている場合があります．環のイデアルは，$\langle 2\rangle$ や $\langle x, y\rangle$ のように，生成元を普通の丸括弧で囲むのではなく角括弧で囲むことで表現しています．集合 A, B に対して $A \subset B$ は真の包含関係を表し，$A = B$ の場合を含みません．また，構造を保った部分集合は単に $\subseteq$ で表すのではなく $\leq$ で表します．例えば，$A \leq B$ と書いてあって B が体であれば，A は B の単なる部分集合であるだけではなく，A は B の部分体であることまで含意します．

2. 2016 年 9 月 27 日

2.1. 体の基本

定義 1. K は単位元をもつ可換環で $\langle 0\rangle$ が極大イデアルになることであるとき，K を**体**でいう．

可換環 K において，$\langle 0\rangle$ が極大イデアルであれば，まず極大イデアルは全体ではないことから $1 \notin \langle 0\rangle$ すなわち $0 \neq 1$ が分かる．また，$x \in K$ を 0 でない元とすると，$\langle 0\rangle \leq \langle x\rangle$ が成り立つが，$\langle 0\rangle$ の極大性から $\langle x\rangle = K$ となるので，ある $y \in K$ で $xy = 1$ となるものが存在する．すなわち，任意の 0 でない元は乗法に関する逆元をもつ．

可換環 A に対してその極大イデアル $\mathfrak{m}$ をとると $A/\mathfrak{m}$ は体になる．特に，体 K に対し，多項式環 $K[X]$ の極大イデアルは既約多項式 (特にモニックであるとして良い) で生成されるものであるから，既約多項式 $P \in K[X]$ に対して $K[X]/\langle P\rangle$ は体である．例えば，$\mathbb{R}[X]$ において $X^2 + 1$ は既約だから，

$$\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$$

は実際に体になっている．

体 K をとると，環の準同型写像 $\varphi\colon \mathbb{Z} \to K$ は唯一定まる．実際，$\varphi(1) = 1_K$ だから，準同型性から $\varphi(n)$ は 1_K を n 回たしたものにならざるを得ない．このとき，準同型定理によって $\mathbb{Z}/\operatorname{Ker}\varphi$ は K の部分環 $L := \operatorname{Im}\varphi$ と同型であるが，K は体より特に整域なので，L も整域となり $\mathbb{Z}/\operatorname{Ker}\varphi$ も整域である．したがって，$\operatorname{Ker}\varphi$ は $\mathbb{Z}$ の素イデアルであるから，ある素数 p によって $\operatorname{Ker}\varphi = \langle p\rangle$ と書けるか，$\operatorname{Ker}\varphi = \langle 0\rangle$ である．ここで，以下の定義が意味をもつ．

定義 2. 体 K に対し，環の準同型写像 $\varphi\colon \mathbb{Z} \to K$ をとる．$\mathrm{Ker}\,\varphi = \langle p \rangle$ を満たす素数もしくは 0 である p を，K の**標数**といい $\mathrm{char}\,K$ で表す．

命題 1. 体 K の標数を p とする．$p > 0$ ならば，K は $\mathbb{Z}/p\mathbb{Z}$ と同型な体を含む．$p = 0$ ならば，K は $\mathbb{Q}$ と同型な体を含む．

$p > 0$ であれば，上で述べた環の準同型写像 $\varphi\colon \mathbb{Z} \to K$ について，準同型定理によって $\mathrm{Im}\,\varphi \cong \mathbb{Z}/p\mathbb{Z}$ である．$\mathrm{Im}\,\varphi \subseteq K$ だから，命題の主張が示された．$p = 0$ であれば，$\mathrm{Im}\,\varphi \cong \mathbb{Z}$ であるから K は $\mathbb{Z}$ と同型な部分環を含む．$\mathbb{Z}$ の商体は $\mathbb{Q}$ であるから K は $\mathbb{Q}$ と同型な体も含み，この場合も命題の主張が示された．

定義 3. 体 K の標数を p とし，$p > 0$ であるとする．このとき，体の準同型写像

$$\varphi\colon\ K \to K;\ x \mapsto x^p$$

を **Frobenius 写像**と呼ぶ．$\mathrm{Im}\,\varphi$ を K^p と書く．

体 K, L の間の準同型写像 $\varphi\colon K \to L$ があると，$\mathrm{Ker}\,\varphi$ は K のイデアルである．体のイデアルは 0 から全体だが，$\varphi(1) = 1$ より $\mathrm{Ker}\,\varphi \neq K$ であるから，$\mathrm{Ker}\,\varphi = 0$ である．したがって，φ は単射となる．よって，K と $\varphi(K) \leq L$ を同一視することで，K は L の部分であると見なせる．

定義 4. 体 K, L の間に準同型写像 $\varphi\colon K \to L$ があるとき，L を K の**拡大体**といい，K を L の**部分体**という．この関係があるとき L/K と表す．

定義 5. 体の拡大 L/K を考える．K を含む L の部分体を拡大 L/K の**中間体**という．

以下では，K が L の部分体であるとき，上で述べた同一視によって $K \subseteq L$ であるかのように議論を進めることがある．

2.2. 代数拡大と超越拡大

体の拡大 L/K を考え，$x \in L$ をとる．

$$\varphi_x\colon\ K[X] \to L;\ f \mapsto f(x)$$

とおくと，$\mathrm{Ker}\,\varphi_x$ は $K[X]$ の素イデアルになるから，あるモニック既約多項式 $P \in K[X]$ によって $\mathrm{Ker}\,\varphi_x = \langle P \rangle$ と書けるか，$\mathrm{Ker}\,\varphi = \langle 0 \rangle$ である．したがって，以下の定義が意味をもつ．

定義 6. 体の拡大 L/K を考え，$x \in L$ をとる．

$$\varphi_x\colon\ K[X] \to L;\ f \mapsto f(x)$$

とおくと，これは体の準同型写像である．あるモニック多項式 P によって $\mathrm{Ker}\,\varphi_x = \langle P \rangle$ と書けるとき，x は K 上**代数的**であるといい，P を x の K 上**最小多項式**という．$\mathrm{Ker}\,\varphi_x = \langle 0 \rangle$ のときは，x は

K 上**超越的**であるという．

要するに，$x \in L$ が代数的とは，x が K 上多項式の根になっているということである．x を根にもつ K 上多項式のうち，次数が最小で最大次の係数が 1 のものが x の最小多項式である．

定義 7. 体の拡大 L/K を考える．L の任意の元が K 上代数的であるとき，L を K の**代数拡大**という．そうでないとき，L を K の**超越拡大**という．

しばらくの間，代数的な元について考える．体の拡大 L/K を考え，$x \in L$ をとる．x が K 上代数的なら，上記で定義した φ_x に対して，準同型定理によって $K[X]/\langle P\rangle \cong \mathrm{Im}\,\varphi_x$ が成り立つ．$K[X]/\langle P\rangle$ は体だから，$\mathrm{Im}\,\varphi_x$ も体となる．

定義 8. 体の拡大 L/K を考え，$x \in L$ は K 上代数的であるとする．このとき，上記の記号での体 $\mathrm{Im}\,\varphi_x \leq L$ を x によって K 上**生成される部分体**といい $K(x)$ で表す．また，x を $K(x)$ の**生成元**という．

1 の原始 3 乗根 $\omega = (1+\sqrt{-3})/2$ をとる．

$$\varphi\colon\ \mathbb{R}[X] \to \mathbb{C};\ f \mapsto f(\omega)$$

とすると，$\omega^2+\omega+1=0$ だから，少なくとも $\mathrm{Ker}\,\varphi \supseteq \langle X^2+X+1\rangle$ が成り立つ．$X^2+X+1 \in \mathbb{R}[X]$ が既約であることが示されれば，この包含関係は等号となる．これを示す．まず，φ は環の準同型写像

$$\tilde{\varphi}\colon\ \mathbb{R}[X]/\langle X^2+X+1\rangle \to \mathbb{C};\ \overline{f} \mapsto f(\omega)$$

を誘導する．ここで，$\mathbb{R}[X]/\langle X^2+X+1\rangle$ と $\mathbb{C}$ はともに $\mathbb{R}$-線型空間としての構造をもち，$\tilde{\varphi}$ は $\mathbb{R}$-線型写像にもなっている．$\dim_{\mathbb{R}} \mathbb{C} = 2$ であって，1 と ω は明らかに $\mathbb{C}$ 上線型独立なので，線型空間として $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\omega$ となる．この基底について $1 = \tilde{\varphi}(\overline{1})$, $\omega = \tilde{\varphi}(\overline{X})$ が成り立つから，$\tilde{\varphi}$ は全射である．また，$\dim_{\mathbb{R}} \mathbb{R}[X]/\langle X^2+X+1\rangle = 2$ も容易に分かる．したがって，$\tilde{\varphi}$ は次元が有限で等しい線型空間の間の全射線型写像だから，同型写像になる．これより，$\tilde{\varphi}$ は環の間の写像としても同型写像である．$\mathbb{C}$ は体だから，$\mathbb{R}[X]/\langle X^2+X+1\rangle$ も体となり，$\langle X^2+X+1\rangle$ は極大イデアルだから X^2+X+1 は既約である．さて，これにより ω の最小多項式は X^2+X+1 で，$\mathbb{R}(\omega) = \mathbb{C}$ が分かった．

多項式の既約性の判定には以下の定理が知られている．

定理 2.［Eisenstein の既約性判定法］ 主イデアル整域 A に対し，$P \in A[X]$ をとる．

$$P =: X^n + a_1 X^{n-1} + \cdots + a_n$$

とおくとき，A のある素元 π が存在して，π は各 a_i をわり切り，π^2 は a_n をわり切らないとする．このとき，A の分数体を K とすれば，P は $K[X]$ 上既約である．

例えば，$X^3-2 \in \mathbb{Z}[X]$ を考えると，$\mathbb{Z}$ において各係数 0, -2 はともに 2 でわり切れるが -2 は $2^2=4$ ではわり切れない．$\mathbb{Z}$ の分数体は $\mathbb{Q}$ だから，これより X^3-2 は $\mathbb{Q}[X]$ で既約である．したがって，こ

の根の 1 つである $\sqrt[3]{2}$ の最小多項式が $X^3 - 2$ であることが分かる．

さて，体の拡大 L/K を考え，$x \in L$ は K 上超越的であるとする．上で定義した φ_x は体の準同型写像

$$\tilde{\varphi}_x\colon\ K(X) \mapsto L;\ \frac{f}{g} \mapsto \frac{f(x)}{g(x)}$$

を引き起こす．x の超越性から $\mathrm{Ker}\,\varphi_x = 0$ だったから，$\mathrm{Ker}\,\tilde{\varphi}_x = 0$ となり $\tilde{\varphi}_x$ は単射である．したがって，$\mathrm{Im}\,\tilde{\varphi}_x$ は体になる．

定義 9. 体の拡大 L/K を考え，$x \in L$ は K 上代数的であるとする．このとき，上記の記号での体 $\mathrm{Im}\,\tilde{\varphi}_x \leq L$ を x によって K 上**生成される部分体**といい $K(x)$ で表す．また，x を $K(x)$ の**生成元**という．

以上によって，体の拡大 L/K があるとき $x \in L$ が代数的である場合にも超越的である場合にも $K(x)$ が定義された．実は，以下の意味で 2 種類の $K(x)$ は同じ性質をもつ．

命題 3. 体の拡大 L/K を考え，$x \in L$ をとる．$K(x)$ は x を属する最小の K の拡大体である．

証明は適当な本に載っているはずである．

生成される部分体のこの性質から，生成元が複数個の場合に拡張される．

定義 10. 体の拡大 L/K を考え，部分集合 $S \subseteq L$ をとる．S を含む最小の K の拡大体を S によって K 上**生成される部分体**といい $K(S)$ で表す．$S =: \{x_1, \cdots, x_n\}$ であるときは，$K(S)$ を $K(x_1, \cdots, x_n)$ で表す．

3. 2016 年 10 月 4 日

3.1. 拡大次数

体の拡大 L/K があるとき，K の積をスカラー倍と見なすことで L は K-線型空間と見なせる．

定義 11. 体の拡大 L/K において，K-線型空間としての L の次元を L の K 上**拡大次数**といい，$[L : K]$ で表す．$[L : K] < \infty$ のとき，L は K の**有限次拡大**という．

例えば，$[\mathbb{C} : \mathbb{R}] = 2$ や $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 3$ である．また，体の拡大 L/K において，$x \in L$ が K 上代数的で，P をその最小多項式とすると，$K(x) \cong K[X]/\langle P \rangle$ だから，$[K(x) : K] = \deg P$ である．

命題 4. 体の拡大 L/K, M/L があるとき，M は K の拡大体と見なせて，

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

が成り立つ．

$m \coloneqq [M : L]$, $n \coloneqq [L, K]$ とおくと，$m, n < \infty$ であれば，

$$M \cong L^{\oplus m};\quad L \cong K^{\oplus n}$$

が成り立つ．したがって，

$$M \cong (K^{\oplus n})^{\oplus m} \cong K^{\oplus mn}$$

なので，M の K-線型空間としての次元は mn である．したがって，命題の等式が示された．m, n の一方が ∞ となる場合も同様である．

命題 5. 体の拡大 L/K と $x \in L$ に対し，

[1] x は K 上代数的である
[2] x を属する L の部分体で K 上有限次拡大であるものが存在する

は同値である．

[1]⇒[2]: x の最小多項式を $P \in K[X]$ とすると，$x \in K(x)$ であって $[K(x) : K] = \deg P < \infty$ である．したがって，$K(x)$ を考えれば良い．
[2]⇒[1]: 条件 2 の有限次拡大を M とする．

$$\varphi\colon\ K[X] \mapsto M;\ f \mapsto f(x)$$

とおくと，これは環準同型写像であり，また K-線型写像でもある．M は K 上有限次元で，$K[X]$ は K 上無限次元なので，φ は単射ではあり得ない．したがって，$\mathrm{Ker}\,\varphi \neq 0$ なので，あるモニック既約多項式 $P \in K[X]$ によって $\mathrm{Ker}\,\varphi = \langle P \rangle$ と書ける．これは，x が K 上代数的であることを意味する．

命題 6. 体の拡大 L/K が有限次拡大であれば，代数拡大である．

任意の $x \in L$ をとったとき，命題 5 の条件 2 における K 上有限次拡大を L 自身にとれば良い．
さて，体の部分環が再び体となる十分条件として，以下のことが知られている．

補題 7. 体の拡大 L/K に対し，$M \leq L$ は K を含む部分環であって K-線型空間として有限次元であるとする．このとき，M は体になる．

0 でない元 $x \in M$ をとる．

$$h_x\colon\ M \to M;\ a \mapsto ax$$

を考えると，これは体の準同型写像かつ K-線型写像である．M が特に整域だから，$\mathrm{Ker}\,h_x = 0$ となって h_x は単射である．また M は有限次元だから，h_x は同じ有限次元線型空間の間の単射線型写像なので，同型写像である．したがって，$h^{-1}(1) \in M$ が存在し，これが x の乗法に関する逆元を与える．x は 0 でない任意の元にとれるから，M は体である．

命題 8. 体の拡大 L/K において，$x, y \in L$ が K 上代数的であるとする．このとき，$f \in K[X, Y]$ に対して $f(x, y)$ も K 上代数的である．

環の準同型写像

$$\varphi\colon\ K[X, Y] \to L;\ g \mapsto g(x, y)$$

をとる．また，$P \in K[X]$ と $Q \in K[Y]$ をそれぞれ x, y の最小多項式とする．このとき，$P, Q \in \operatorname{Ker}\varphi$ である．したがって，φ は環の準同型写像

$$\tilde{\varphi}\colon\ K[X, Y]/\langle P, Q\rangle \to L;\ \overline{g} \mapsto g(x, y)$$

を引き起こす．$M \coloneqq \operatorname{Im}\tilde{\varphi}$ とすると，$f(x, y) = \varphi(\overline{f})$ だから，$f(x, y) \in M$ である．

$m \coloneqq \deg P$, $n \coloneqq \deg Q$ とすると，

$$\{\overline{X^i Y^j} \mid 0 \le i < m,\ 0 \le j < n\}$$

は $K[X, Y]/\langle P, Q\rangle$ の K-基底となるから，$K[X, Y]/\langle P, Q\rangle$ は特に有限次元である．したがって，$\tilde{\varphi}$ によるその像 M も有限次元であり，すなわち M は K の有限次拡大である．さらに，補題 7 によって M は体になるから，命題 5 の条件 2 が満たされ，$f(x, y)$ は K 上代数的である．

3.2. 合成体

定義 12. 体の拡大 L/K とその中間体 M_1, M_2 に対し，$K(M_1 \cup M_2)$ を M_1 と M_2 の**合成体**といい $M_1 \cdot M_2$ で表す．

体の拡大 $\mathbb{R}/\mathbb{Q}$ を考え，その中間体として $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{3})$ をとる．このとき，

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$$

が成り立つ．$\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{3})$ の合成体は，この 2 つと $\mathbb{Q}$ を含む最小の体だから $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ である．ここで，$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ が成り立つから $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}(\sqrt{2})$ である．したがって，$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \neq 1$ である．さらに，$X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ は $\sqrt{3}$ を根にもつので，$\sqrt{3}$ の $\mathbb{Q}(\sqrt{2})$ 上最小多項式は 2 次以下である．すなわち，$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \le 2$ が分かる．以上により，$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ である．よって，

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

となる．$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ は $\mathbb{Q}$ 上線型独立な $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の元であり，上の式より $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ 上 4 次元なので，これらは基底をなし，

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$$

が成り立つ．一方，$1,\ \sqrt{2}+\sqrt{3},\ 5+2\sqrt{6}$ は $\mathbb{Q}$ 上線形独立で，$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ なので，これらは全て $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ の元である．したがって，$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \geq 3$ が成り立つ．ここで，

$$[\mathbb{Q}(\sqrt{2},\ \sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})][\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\ \sqrt{3}) : \mathbb{Q}] = 4$$

だから，右辺は $1\cdot 4$ か $2\cdot 2$ か $4\cdot 1$ のいずれかである．しかし，$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \geq 3$ であったから，$[\mathbb{Q}(\sqrt{2},\ \sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 1$ である．すなわち，$\mathbb{Q}(\sqrt{2},\ \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ が分かった．

4. 2016 年 10 月 11 日

4.1. 準同型写像の個数と最小多項式の分解

定義 13. 体 K とその拡大体 $L,\ K'$ をとる．体の準同型写像 $f\colon L \to K'$ が $f|_K = \mathrm{id}_K$ を満たすとき，f を **K-準同型写像**という．L から K' への K-準同型写像全体を $\mathrm{Mor}_K(L,\ K')$ と書く．

明らかに $\mathrm{Mor}_K(L,\ K') \subseteq \mathrm{Hom}_K(L,\ K')$ が成り立つ [*1]．

補題 9. 体 K とその拡大体 $L,\ K'$ をとり，ある $x \in L$ によって $L = K(x)$ と表せるとする．x の最小多項式を $P \in K[X]$ とするとき，

$$\#\{y \in K' \mid P(y) = 0\} = \#\,\mathrm{Mor}_K(L,\ K')$$

が成り立つ．

$L = K(x)$ だから，$L = K[X]/\langle P\rangle$ と見なせる．また，

$$S \coloneqq \{y \in K' \mid P(y) = 0\}$$

とおく．$\sigma \in \mathrm{Mor}_K(L,\ K')$ に対し，$y \coloneqq \sigma(\overline{X}) \in L$ とする．

$$P =: \sum_{i=1}^{n} a_i X^i \quad (a_i \in K)$$

と表せば，$\overline{P} = 0$ であって，σ は K の元を変えないから，

$$0 = \sigma(\overline{P}) = \sigma\left(\sum_{i=1}^{n} \overline{a_i}\overline{X^i}\right) = \sum_{i=1}^{n} \sigma(\overline{a_i})\sigma(\overline{X})^i = \sum_{i=1}^{n} a_i y^i = P(y)$$

を得る．したがって，$y \in S$ が分かった．これより，写像

$$\Phi\colon\ \mathrm{Mor}_K(L,\ K') \to S;\ \sigma \mapsto \sigma(\overline{X})$$

が定義できる．逆に，$y \in S$ に対し，

$$\varphi_y\colon\ K[X] \to K';\ f \mapsto f(y)$$

[*1] $\mathrm{Hom}_K(L,\ K')$ は L から K' への K-線型写像全体を表す．これは K'-線型空間になる．

を考えれば，$P(y) = 0$ だから，

$$\tilde{\varphi}_y\colon\ K[X]/\langle P\rangle \to K';\ \overline{f} \mapsto f(y)$$

が誘導される．これは K-準同型写像になるから，$\tilde{\varphi}_y \in \mathrm{Mor}_K(L,\ K')$ である．これより，写像

$$\Psi\colon\ S \to \mathrm{Mor}_K(L,\ K');\ y \mapsto \tilde{\varphi}_y$$

が定義できた．ここで，Φ と Ψ は互いに逆写像になっているので全単射である．したがって，

$$\#S = \#\,\mathrm{Mor}_K(L,\ K')$$

が成り立つ．

定理 10. 体 K とその拡大体 $L,\ K'$ をとり，L は K の有限次拡大とする．このとき，

$$\#\,\mathrm{Mor}_K(L,\ K') \leq [L : K] \qquad [\heartsuit]$$

が成り立ち，

[1] 式 $\heartsuit$ が等号で成り立つ

[2] L の任意の元の K 上最小多項式は，K' 上で相異なる 1 次式の積に分解する

[3] ある $x_1, \cdots, x_n \in L$ が存在して，$L = K(x_1,\ \cdots,\ x_n)$ が成り立ち，$x_1,\ \cdots,\ x_n$ の各 K 上最小多項式が K' 上で相異なる 1 次式の積に分解する

は同値である．

$\mathrm{Hom}_K(L,\ K')$ を K'-線型空間と見なす．$n := [L : K]$ とすると $L \cong K^{\oplus n}$ であるから，

$$\mathrm{Hom}_K(L,\ K') \cong \mathrm{Hom}_K(K^{\oplus n},\ K') \cong \mathrm{Hom}_K(K,\ K')^{\oplus n} \cong K'^{\oplus n}$$

である．したがって，

$$\dim_{K'} \mathrm{Hom}_K(L,\ K') = [L : K]$$

が成り立つ．これより，$\mathrm{Mor}_K(L,\ K')$ の元が $\mathrm{Hom}_K(L,\ K')$ 上線型独立であることを示せば，線型独立な元の個数は次元以下であることから，式 $\heartsuit$ が示される．

$\sigma_1, \cdots, \sigma_m \in \mathrm{Mor}_K(L,\ K')$ を相異なる元とする．m に関する帰納法で $\sigma_1, \cdots, \sigma_m$ の線型独立性を示す．$m = 1$ のときは示すべきことはない．$m \geq 2$ とする．$\sigma_1, \cdots, \sigma_m$ が線型独立でないと仮定すると，必要ならば添字の順番を入れ替えて，

$$\sigma_m =: \sum_{i=1}^{m-1} a_i \sigma_i \quad (a_i \in K')$$

と書ける．すると，任意の $t \in L$ に対して，この式の両辺に $\sigma_m(t)$ をかけることで，

$$\sigma_m(t)\sigma_m = \sum_{i=1}^{m-1} a_i \sigma_m(t) \sigma_i$$

が成り立つ．また，

$$\sigma_m(t)\sigma_m = \sum_{i=1}^{m-1} a_i\sigma_i(t)\sigma_i$$

も成り立つ． したがって，

$$\sum_{i=1}^{m-1} a_i\sigma_m(t)\sigma_i = \sum_{i=1}^{m-1} a_i\sigma_i(t)\sigma_i$$

を得るが，帰納法の仮定によって $\sigma_1, \cdots, \sigma_{m-1}$ は線型独立だから，各 i に対して，

$$a_i\sigma_m(t) = a_i\sigma_i(t)$$

が分かる．もしある i で $a_i \neq 0$ なら，上式の両辺に a_i^{-1} をかけることで，任意の $t \in L$ に対して $\sigma_m(t) = \sigma_i(t)$ を得るが，これは σ_m と σ_i が異なるということに矛盾する．したがって，全ての i で $a_i = 0$ である．すると σ_m は零写像になるが，零写像は体の準同型写像ではないので，これは矛盾である．よって，$\sigma_1, \cdots, \sigma_m$ は線型独立である．

[1]⇒[2]: 任意に $x \in L$ をとる．$M := K(x)$ とおくと，包含写像 $\iota\colon M \to L$ に対して，

$$\begin{array}{ccc} \mathrm{Mor}_K(L,\, K') & \hookrightarrow & \mathrm{Hom}_K(L,\, K') \\ {\scriptstyle \circ\iota}\downarrow & & \downarrow{\scriptstyle \circ\iota} \\ \mathrm{Mor}_K(M,\, K') & \hookrightarrow & \mathrm{Hom}_K(M,\, K') \end{array}$$

は可換である [*2]．また，条件 1 から，

$$\#\,\mathrm{Mor}_K(L,\, K') = [L : K] = \dim_{K'} \mathrm{Hom}_K(L,\, K')$$

が成り立つので，上で述べたように $\mathrm{Mor}_K(L,\, K')$ は $\mathrm{Hom}_K(L,\, K')$ 上線型独立だったから，基底になる．同様に，$\mathrm{Mor}_K(M,\, K')$ は $\mathrm{Hom}_K(M,\, K')$ 上線型独立である．さらに上の可換性から，$\mathrm{Mor}_K(M,\, K')$ は $\mathrm{Hom}_K(M,\, K')$ を生成する． 線型独立な生成系は基底だから，これによって，

$$\#\,\mathrm{Mor}_K(M,\, K') = \dim_{K'} \mathrm{Hom}_K(M,\, K') = [M : K]$$

を得る．

ここで，x の K 上最小多項式を P とすれば，$M = K[X]/\langle P\rangle$ と見なせる．さらに，

$$S := \{y \in K' \mid P(y) = 0\}$$

とおけば，補題 9 によって，

$$\#S = \#\,\mathrm{Mor}_K(M,\, K')$$

が成り立つ．P を K' 上の多項式であると見なし，これを 1 次式でわれるだけわって，

$$P =: (X - a_1)(X - a_2)\cdots(X - a_k)Q \quad (a_i \in K',\, Q \in K'[X])$$

[*2] $\circ\iota$ は，ι を前に合成する写像，すなわち f を $f \circ \iota$ に移す写像を表す．

と表す．$y \in S$ をとると，$P(y) = 0$ だから，

$$(y - a_1)(y - a_2) \cdots (y - a_k)Q(y) = 0$$

であるが，$Q(y) \neq 0$ であるから，y は $a_1, \cdots, a_k$ のいずれかと等しい．したがって，

$$\#S \leq k \leq \deg P \qquad [\sharp]$$

を得る．一方で，これまでの議論によって，

$$\#S = \#\mathrm{Mor}_K(M, K') = [M : K] = \deg P$$

が分かっているから，結局式 $\sharp$ は等号で成り立つ．すなわち，$\#S = k$ であることから $a_1, \cdots, a_k$ は相異なり，$k = \deg P$ であることから $Q = 1$ でなければならない．これは条件 2 の主張そのものである．

[2]⇒[3]: L は K の有限次拡大だから，L の K-基底 $x_1, \cdots, x_n \in L$ がとれる．これらは特に L を体としても生成するから，$L = K(x_1, \cdots, x_n)$ である．また，条件 2 から $x_1, \cdots, x_n$ の各最小多項式は K' で相異なる 1 次式の積に分解する．したがって，条件 3 が示された．

[3]⇒[1]: n に関する帰納法により示す．$n = 1$ であれば $L = K(x_1)$ であるから，x_1 の K 上最小多項式を P とし，

$$S \coloneqq \{y \in K' \mid P(y) = 0\}$$

とおけば，補題 9 によって，

$$\#S = \#\mathrm{Mor}_K(L, K')$$

が成り立つ．条件 3 によって，P は $K'[X]$ の元として

$$P =: (X - a_1)(X - a_2) \cdots (X - a_k) \quad (a_i \in K')$$

と分解でき，$a_1, \cdots, a_k$ は相異なる．したがって，

$$\#S = k = \deg P = [L : K]$$

であるから，結局

$$\#\mathrm{Mor}_K(L, K') = [L : K]$$

が成り立ち，条件 1 が成立する．

$n \geq 2$ とする．$M \coloneqq K(x_n)$ とおくと，$L = M(x_1, \cdots, x_{n-1})$ である．まず $M \coloneqq K(x_n)$ なので，上の場合の議論によって，

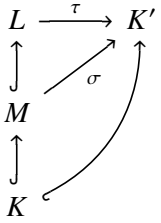
$$\#\mathrm{Mor}_K(M, K') = [M : K]$$

が成り立つ．ここで，$\sigma \in \mathrm{Mor}_K(M, K')$ を 1 つとり固定する．これにより，K' は M の拡大体と見なせる．各 x_i $(1 \leq i \leq n-1)$ の K 上最小多項式を $P_i \in K[X]$ とし，M 上最小多項式を $Q_i \in M[X]$ とす

る．$M \geq K$ だから，Q_i は P_i をわり切る．条件 3 により P_i は K' 上で相異なる 1 次式の積に分解するから，それをわり切る Q_i も K' 上で相異なる 1 次式の積に分解する．つまり，$x_1, \cdots, x_{n-1}$ の各 M 上最小多項式は K' 上で相異なる 1 次式の積に分解する．よって，帰納法の仮定を用いると，

$$\#\mathrm{Mor}_M(L, K') = [L : M]$$

が得られる．今，σ によって K' を M の拡大体と見ているので，$\mathrm{Mor}_M(L, K')$ の元というのは，図式



において，M, L, K' から成る三角形部分を可換にするような体の準同型写像 τ のことである．これは，上の議論によって $[L : M]$ 個あることが分かっている．また，$\mathrm{Mor}_K(M, K')$ の元というのは，上の図式の K, M, K' から成る三角形部分を可換にするような体の準同型写像 σ のことで，これは $[M : K]$ 個あることが分かっている．$\mathrm{Mor}_K(L, K')$ の元は，上の図式の K, L, K' から成る三角形部分を可換にするような τ のことで，以上の議論によって，これは $\mathrm{Mor}_K(M, K')$ の元と $\mathrm{Mor}_M(L, K')$ の元を定めれば 1 つ定まる．したがって，

$$\#\mathrm{Mor}_K(L, K') = \#\mathrm{Mor}_M(L, K') \cdot \#\mathrm{Mor}_K(M, K') = [L : M][M : K] = [L : K]$$

が得られた．これより，条件 1 が示された．

なお，後に述べる分離拡大の言葉を用いて，この定理の同値な 3 条件を言い換えることができる．これは定理 25 を参照すること．

5. 2016 年 10 月 25 日

5.1. 根の添加と分解体

定義 14. 体 K と既約多項式 $P \in K[X]$ に対し，$K[X]/\langle P\rangle$ を K に P の**根を添加した体**という．

$x \coloneqq \overline{X} \in K[X]/\langle P\rangle$ とすれば，$K[X]/\langle P\rangle = K(x)$ であり $K[X]/\langle P\rangle$ 上で $P(x) = 0$ が成り立つ．すなわち，どんな多項式であっても，根を添加した体を考えることによって根をもつようにできるということである．

定義 15. 体 K とモニック多項式 $P \in K[X]$ をとる．K の拡大体 K' に対し，$P \in K'[X]$ と見なすと $a_i \in K'$ たちによって，

$$P = \prod_{i=1}^{n} (X - a_i)$$

と 1 次式の積に分解するとき，K' を P の**分解体**という．さらに，$K' = K(a_1, \cdots, a_n)$ であれば，K' を P の**最小分解体**という．

多項式をどの拡大体で分解するかによって，その多項式の分解体が様々に作れることに注意すること．

$P \coloneqq X^3 - 2 \in \mathbb{Q}[X]$ を考えると，これは $\mathbb{C}[X]$ において，

$$P = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\omega)(X - \sqrt[3]{2}\omega^2)$$

と分解する．なお，ω は 1 の原始 3 乗根である．したがって，

$$L \coloneqq \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

は $\mathbb{C}$ 内の P の最小分解体である．

命題 11. 体 K とモニック多項式 $P \in K[X]$ に対し，P の分解体は存在する．

$n \coloneqq \deg P$ に関する帰納法による．$n = 0$ ならば $P = 1$ だから，K そのものが P の分解体になる．

$n \geq 1$ とする．$Q \mid P$ なる既約多項式 $Q \in K[X]$ をとり，$L \coloneqq K[X]/\langle Q \rangle$ とおく．L は K の拡大体だから $P, Q \in L[X]$ と見なすことができ，$x \coloneqq \overline{X} \in L$ とすると $Q(x) = 0$ を満たす．$Q \mid P$ であったから，$P(x) = 0$ も成り立つ．したがって，ある $P_1 \in L[X]$ が存在して $P = (X - x)P_1$ と書ける．$\deg P_1 < \deg P$ だから，帰納法の仮定によって P_1 の L 上分解体 M が存在する．このとき，P_1 は $M[X]$ において 1 次式の積に分解するから，$P = (X - x)P_1$ も $M[X]$ で 1 次式の積に分解する．よって，M は P の分解体でもある．

命題 12. 体 K とモニック多項式 $P \in K[X]$ をとる．P の最小分解体 L および K の拡大体 K' に対し，

[1] K' は P の K 上分解体である

[2] 体の K-準同型写像 $\varphi\colon L \to K'$ が存在する

は同値である．

[1]⇒[2]: $n \coloneqq \deg P$ に関する帰納法による．$n = 0$ なら $P = 1$ だから，$L = K$ である．したがって，$\varphi\colon L \to K'$ を包含写像とすれば良い．

$n \geq 1$ とする．$Q \mid P$ なる既約多項式 $Q \in K[X]$ をとる．L は P の分解体なので，P は $L[X]$ において 1 次式の積に分解するから，それをわり切る Q も $L[X]$ で 1 次式の積に分解する．したがって，ある $a \in L$ が存在して $Q(a) = 0$ が成り立つ．$K_1 \coloneqq K(a) \leq L$ とすると，

$$\psi\colon\ K[X]/\langle Q \rangle \to K_1;\ \overline{f} \mapsto f(a)$$

は定義できて体の準同型写像となり，さらに全射である．体の準同型写像は勝手に単射になるので，ψ は同型写像である．よって，以降は $K_1 = K[X]/\langle Q \rangle$ と見なす．さて，K' は P の分解体なので，P は

$K'[X]$ で 1 次式の積に分解し，したがって Q も 1 次式の積に分解する．よって，ある $x \in K'$ がとれて $Q(x) = 0$ が成り立つ．これにより，

$$\psi' \colon\ K[X]/\langle Q\rangle \to K';\ \overline{f} \mapsto f(x)$$

が定義てきて体の K-準同型写像になる．この ψ' によって $K_1 = K[X]/\langle Q\rangle$ を K' の部分体と見なす．

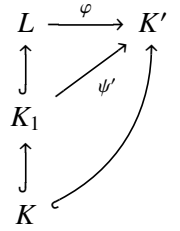
P の $L[X]$ における 1 次式の分解は，$P(a) = 0$ だったことを踏まえると，$a_i \in L$ たちによって，

$$P =: (X - a)\prod_{i=0}^{n-1}(X - a_i)$$

と表せる．また，$a \in K_1$ より $P = (X - a)P_1$ を満たす $P_1 \in K_1[X]$ がとれて，$L[X]$ においては

$$P_1 = \prod_{i=0}^{n-1}(X - a_i)$$

と分解される．ここで，L は最小分解体だから $L = K(a_1, \cdots, a_{n-1}, a)$ である．$K_1 = K(a)$ とおいたから，$L = K_1(a_1, \cdots, a_{n-1})$ でもある．すなわち，L は P_1 の K_1 上最小分解体である．さらに，K' は P の K 上分解体であったから P_1 の K 上分解体にもなっている．以上により帰納法の仮定が使えて，体の K_1-準同型写像 $\varphi \colon L \to K'$ が存在する．さて，今は ψ' によって $K_1 \leq K$ と見なしているから，図式



は可換である．したがって，φ は K-準同型写像にもなっており，これが存在を示したいものであった．

[2]⇒[1]:　K-準同型写像 $\varphi \colon L \to K'$ があれば，これによって L は K' の部分体と見なせる．L は P の K 上分解体だから，その拡大体 K' も P の分解体である．

命題 13.　体 K とモニック多項式 $P \in K[X]$ をとる．また，P の最小分解体 L および K の拡大体 K' をとる．K' 内の P の最小分解体は，命題 12 の条件 2 の準同型写像 $\varphi \colon L \to K'$ の像に一致する．

L と K' は P の分解体だから，$a_i \in L$ たちと $b_i \in K'$ たちによって，

$$P = \prod_{i=1}^{n}(X - a_i) = \prod_{i=1}^{n}(X - b_i)$$

と分解される．φ は多項式環の間の準同型写像 $\hat{\varphi} \colon L[X] \to K'[X]$ を誘導するが，f は K の元を変えないから $\hat{f}(P) = P$ が成り立つ．一方，上の表示において，

$$\hat{\varphi}(P) = \prod_{i=1}^{n}(X - \varphi(a_i))$$

が成り立つ．これによって，$K'[X]$ における P の 2 通りの表示

$$P = \prod_{i=1}^{n}(X - \varphi(a_i)) = \prod_{i=1}^{n}(X - b_i)$$

が得られたので，$\varphi(a_1), \cdots, \varphi(a_n)$ と $b_1, \cdots, b_n$ は順番を入れ替えればそれぞれ一致していなければならない．$L = K(a_1, \cdots, a_n)$ だから，

$$\varphi(L) = K(\varphi(a_1), \cdots, \varphi(a_n)) = K(b_1, \cdots, b_n)$$

が成り立つ．この右辺は K' 内の P の最小分解体だから，命題が従う．

定理 14. 体 K とモニック多項式 $P \in K[X]$ に対し，P の最小分解体は一意に存在する．

命題 11 によって最小分解体の存在は保証されている．さらに命題 13 によって，それらは全て同型であることが分かる．

例として $P := (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ を考える．これは $\mathbb{R}[X]$ においては，

$$P = (X - \sqrt{2})(X + \sqrt{2})(X - \sqrt{3})(X + \sqrt{3})$$

と分解する．したがって，

$$L := \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

が P の最小分解体である．拡大次数は前に見たように $[L : \mathbb{Q}] = 4$ である．

次に $P := X^n - 1 \in \mathbb{Q}[X]$ $(n \geq 1)$ を考える．ζ_n を 1 の原始 n 乗根とすれば，これは $\mathbb{C}[X]$ において，

$$P = \prod_{i=0}^{n-1}(X - {\zeta_n}^i)$$

と分解する．したがって，

$$L := \mathbb{Q}(1, \zeta_n, \cdots, {\zeta_n}^{n-1}) = \mathbb{Q}(\zeta_n)$$

が P の最小分解体である．この拡大次数 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は，1 以上 n 以下の整数の中で n と互いに素なものの個数に一致することが知られている．別の表現をすれば，$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#(\mathbb{Z}/n\mathbb{Z})^\times$ が成り立つ．このことは後に定理 47 として証明する．

T を不定元とする有理関数体 $K := \mathbb{Q}(T)$ を考え，この上の多項式 $P := X^n - T \in K[X]$ $(n \geq 1)$ を考える．ここで，

$$\varphi\colon\ \mathbb{C}[T] \to \mathbb{C}[S];\ T \mapsto S^n$$

は環の準同型写像を定める．φ は単射だから，体の準同型写像

$$\tilde{\varphi}\colon\ \mathbb{C}(T) \to \mathbb{C}(S);\ \frac{f(T)}{g(T)} \mapsto \frac{f(S^n)}{g(S^n)}$$

を誘導する．この写像によって $\mathbb{C}(T) \leq \mathbb{C}(S)$ と見なす．したがって，$\mathbb{Q}(T) \leq \mathbb{C}(T) \leq \mathbb{C}(S)$ という体の拡大列ができる．このとき，P は $\mathbb{C}(S)$ において

$$P = \prod_{i=0}^{n-1} (X - \zeta_n{}^i S)$$

と 1 次式の積に分解される．したがって，

$$L \coloneqq K(S, \zeta_n S, \cdots, \zeta_n{}^{n-1} S) = \mathbb{Q}(S, \zeta_n)$$

が P の最小分解体となる．この拡大次数は，

$$[L : K] = [\mathbb{Q}(S, \zeta_n) : \mathbb{Q}(S)][\mathbb{Q}(S) : \mathbb{Q}(T)] = \#(\mathbb{Z}/n\mathbb{Z})^\times \cdot n$$

である．なお，上記のように $\mathbb{C}(T) \leq \mathbb{C}(S)$ と見なしたとき，しばしば S は $\sqrt[n]{T}$ と書かれる．

5.2. 共役

定義 16. 体 K とその拡大体 L, K' をとり，$a \in L$ とする．a が K 上代数的であるとし，その最小多項式を $P \in K[X]$ とする．このとき，$x \in K'$ が $P(x) = 0$ を満たすならば，x は a の**共役**であるという．さらに，K' が P の分解体となるとき，K' は a の**共役を全て属する**という．

$\mathbb{Q}$ とその拡大体 $L \coloneqq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ を考える．$\sqrt{2} \in L$ の $\mathbb{Q}$ 上最小多項式は $P \coloneqq X^2 - 2$ であり，これは L において，

$$P = (X - \sqrt{2})(X + \sqrt{2})$$

と分解されるから，$\sqrt{2}, -\sqrt{2} \in L$ が $\sqrt{2}$ の共役である．

$\mathbb{Q}$ とその拡大体 $L \coloneqq \mathbb{Q}(\zeta_n)$ を考える．なお，ζ_n は 1 の原始 n 乗根とする．$\zeta_n \in L$ の L での共役は，$\zeta_n{}^i \in L$ $(i \in (\mathbb{Z}/n\mathbb{Z})^\times)$ であることが知られている．

$\mathbb{Q}(T)$ とその拡大体 $L \coloneqq \mathbb{Q}(\sqrt[n]{T}, \zeta_n)$ を考える．$\sqrt[n]{T} \in L$ の $\mathbb{Q}(T)$ 上最小多項式は，Eisenstein の既約性判定法によって $P \coloneqq X^n - T$ であることが分かる．これは L において，

$$P = \prod_{i=0}^{n-1} (X - \zeta_n{}^i \sqrt[n]{T})$$

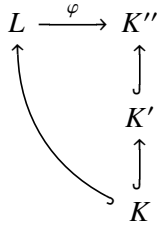
と分解されるのであった．したがって，$\zeta_n{}^i \sqrt[n]{T} \in L$ $(0 \leq i \leq n-1)$ が $\sqrt[n]{T} \in L$ の共役である．

命題 15. 体 K，および K の有限次拡大体 L と K の拡大体 K' をとる．このとき，

[1] 任意の $a \in L$ に対し，K' は a の共役を全て属する

[2] ある $a_1, \cdots, a_n \in L$ が存在して $L = K(a_1, \cdots, a_n)$ を満たし，さらにある $P_1, \cdots, P_n \in K[X]$ が存在して $P_1(a_1) = \cdots = P_n(a_n) = 0$ であって，これらは $K'[X]$ の元と見なすと 1 次式の積に分解できる

[3] K' の拡大体 K'' と体の準同型写像 $\varphi\colon L \to K''$ が図式



を可換にするならば，$\varphi(L) \subseteq K'$ が成り立つ

は同値である．さらに，上の条件が成り立つとき，ある K-準同型写像 $\psi\colon L \to K'$ が存在する．

[1]⇒[2]:　L は K の有限次拡大だから，$L = (a_1, \cdots, a_n)$ を満たすような $a_1, \cdots, a_n \in L$ がとれる．さらに，$a_1, \cdots, a_n$ の K 上最小多項式をそれぞれ $P_1, \cdots, P_n$ とする．明らかに，各 i に対して $P_i(a_i) = 0$ が成り立つ．また，条件 1 から K' は a_i の共役を全て属するから，K' は P_i の分解体となり，P_i は $K'[X]$ において 1 次式の積に分解する．以上により，条件 2 が従う．

[2]⇒[3]:　K' の拡大体 K'' と体の準同型写像 $\varphi\colon L \to K''$ が条件 3 の図式を可換にしているとする．条件 2 から，各 i に対して，L において $P_i(a_i) = 0$ が成り立つ．図式の可換性によって φ は K の元を変えないから，K'' において，

$$P_i(\varphi(a_i)) = \varphi(P_i(a_i)) = 0$$

が成り立つ．ここで，P_i は $K'[X]$ において 1 次式の積に分解するから，ある $b_{ij} \in K'$ たちによって，

$$P_i = \prod_{j=1}^{n_i} (X - b_{ij})$$

と表せる．したがって，上の式と合わせれば，各 i に対してある j が存在して $\varphi(a_i) = b_{ij}$ が成り立つ．$L = K(a_1, \cdots, a_n)$ であって，その各生成元 a_i は φ によって K' の元に移るのだから，$\varphi(L) \subseteq K'$ が成り立つ．

[3]⇒[1]:　任意に $a \in L$ をとる．a の最小多項式を $P \in K[X]$ とおく．ここで L は K の有限次拡大だから，$L = K(a_1, \cdots, a_n)$ を満たす $a_1, \cdots, a_n \in L$ が存在する．$a_1, \cdots, a_n$ の最小多項式をそれぞれ $P_1, \cdots, P_n \in K[X]$ とする．

$$\tilde{P} \coloneqq PP_1 \cdots P_n \in K[X]$$

とおき，$\tilde{P} \in K'[X]$ と見なしたときのこの分解体を K'' とする．$K''[X]$ において $\tilde{P}$ は 1 次式の積に分解するから，特に P も 1 次式の積に分解する．その分解を，$b_j \in K''$ たちによって

$$P = \prod_{j=1}^{m} (X - b_j)$$

と表すことにする．

j $(1 \leq j \leq m)$ を 1 つとって固定する．ここで，

$$K_0 \coloneqq K(a)$$
$$K_i \coloneqq K(a, a_1, \cdots, a_i) \quad (1 \leq i \leq n)$$

とおくと，L の部分体の列

$$K \leq K_0 \leq K_1 \leq \cdots \leq K_n = L$$

が得られる．体の K-準同型写像 $\varphi_i\colon K_i \to K''$ を以下によって帰納的に定める．

$i = 0$ の場合を考える．P は a の最小多項式だから，$K_0 = K(a) \cong K[X]/\langle P\rangle$ が成り立つ．したがって，$\varphi_0\colon K[X]/\langle P\rangle \to K''$ を定めれば良い．$P(b_j) = 0$ だから，

$$\varphi_0\colon\ K[X]/\langle P\rangle \to K'';\ \overline{f} \mapsto f(b_j)$$

が定義でき，K-準同型写像である．

$i \geq 1$ とし，$\varphi_{i-1}\colon K_{i-1} \to K''$ が定まっていると仮定する．$a_i \in K_i$ の最小多項式を $Q_i \in K_{i-1}[X]$ とすると，K_{i-1} において $P_i(a_i) = 0$ であるから $Q_i \mid P_i$ が成り立つ．これより，$\varphi_{i-1}\colon K_{i-1} \to K''$ は係数にこれを適用することによって $\varphi_{i-1}\colon K_{i-1}[X] \to K''[X]$ に拡張されるが，$\varphi_{i-1}(Q_i) \mid \varphi_{i-1}(P_i)$ も成り立つ．φ_{i-1} は K の元を変えないので，$\varphi_{i-1}(P_i) = P_i$ である．P_i は $K''[X]$ において 1 次式の積に分解されるのであったから，それをわり切る $\varphi_{i-1}(Q_i)$ も 1 次式の積に分解する．その分解を，$c_{ik} \in K''$ たちによって

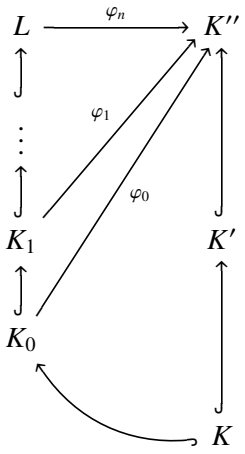
$$\varphi_{i-1}(Q_i) = \prod_{k=1}^{m_i}(X - c_{ik})$$

と表す．さて，$K_i = K_{i-1}(a_i) \cong K_{i-1}[X]/\langle Q_i\rangle$ であることを踏まえて，

$$\varphi_i\colon\ K_{i-1}[X]/\langle Q_i\rangle \to K'';\ \overline{\sum_l d_l X^l} \mapsto \sum_l \varphi_{i-1}(d_l)c_{i1}$$

が定義できる．すなわち，係数に φ_{i-1} を施した多項式に c_{i1} を代入する写像である．φ_{i-1} が K-準同型写像であることから，φ_i も K-準同型写像になる．

以上によって，図式



が得られ，作り方からこれは可換になる．よって，φ_n に条件 3 が適用できるので，$\varphi_n(L) \subseteq K'$ を得る．ところで，作り方から $\varphi_n(a) = b_j$ だから $b_j \in K'$ が分かる．j は任意にとれたので，P の 1 次式の積への分解

$$P = \prod_{j=1}^{m} (X - b_j)$$

は $K'[X]$ における分解にもなるから，K' は P の分解体である．したがって，K' は a の共役を全て属するから，条件 1 が示された．

命題の後半の主張については，上の条件 3 から条件 1 を導いた証明における $\varphi_n\colon L \to K''$ が存在を示したい写像になっている．

命題 15 の条件 3 において，$\iota\colon K' \to K''$ を包含写像とすると，写像

$$I\colon \mathrm{Mor}_K(L, K') \to \mathrm{Mor}_K(L, K'');\ \sigma \mapsto \iota \circ \sigma$$

が定まるが，条件 3 はこの I が全射になることを主張している．一方で，I は自動的に単射になるので，これによって I は全単射になる．

命題 16. 体 K，および K の有限次拡大体 L と K の拡大体 K' をとる．命題 15 の同値な条件が満たされているとき，拡大 L/K の中間体 M に対し，

$$R\colon \mathrm{Mor}_K(L, K') \to \mathrm{Mor}_K(M, K');\ \sigma \mapsto \sigma|_M$$

は全射である．

K, L, K' が，命題 15 の同値な条件のうち特に条件 1 を満たしているとする．このとき，任意の $a \in L$ に対して，a の K 上最小多項式 $P \in K[X]$ は $K'[X]$ において 1 次式の積に分解する．

任意に $\tau \in \mathrm{Mor}_K(M, K')$ をとると，この τ によって K' は M の拡大体と見なすことができる．a の M 上最小多項式を $Q \in M[X]$ とする．$P \in M[X]$ と見なすと $P(a) = 0$ であるから，$Q \mid P$ が成り立つ．P は $K'[X]$ で 1 次式の積に分解できたのだから，それをわり切る Q も 1 次式の積に分解する．したがって，M, L, K' に対しても命題 15 の条件 1 が成り立つ．よって，命題の後半の主張によって，体の M-準同型写像 $\sigma\colon L \to K'$ が存在する．今，τ によって K' を M の拡大体と見ているのだから，図式

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & K' \\ \uparrow & \nearrow_{\tau} & \\ M & & \end{array}$$

は可換である．すなわち，$R(\sigma) = \sigma|_M = \tau$ となるから，R は全射である．

6. 2016 年 11 月 1 日

6.1. 分離多項式

定義 17. 体 K に対し，多項式 $P \in K[X]$ を考える．P の分解体 K' に対して $P \in K'[X]$ が相異なる 1 次式の積に分解できるとき，P を**分離多項式**という．

すなわち，P が分離多項式であるとは P が重根をもたないということである．

定義 18. 体 K 上の多項式

$$P \coloneqq \sum_{i=0}^{n} a_i X^i \quad (a_i \in K)$$

に対し，

$$P' \coloneqq \sum_{i=1}^{n} i a_i X^{i-1}$$

を P の**微分**という．

これは解析学における通常の関数の微分と同じであるから，微分に関する線形性や Leibniz 則は成り立つ．

補題 17. 体 K において，多項式 $P \in K[X]$ と元 $a \in K$ を考える．このとき，

[1] $(X-a)^2 \mid P$ が成り立つ

[2] $X-a \mid P$ および $X-a \mid P'$ が成り立つ

は同値である．

$X-a \mid P$ が成り立つという条件のもとで，$(X-a)^2 \mid P$ と $X-a \mid P'$ が同値であることを示せば良い．まず，$X-a \mid P$ とすると $P=(X-a)Q$ を満たす $Q \in K[X]$ が存在する．このとき，$(X-a)^2 \mid P$ とは $Q(a)=0$ ということである．また，$X-a \mid P'$ とは $P'(a)=0$ ということである．ところが，

$$P' = Q + (X-a)Q'$$

であるから，$Q(a)=P'(a)$ が成り立つ．したがって，$Q(a)=0$ と $P'(a)=0$ は同値であり，補題が示された．

補題 18. 体の拡大 K'/K と多項式 $P, Q \in K[X]$ をとる．このとき，

[1] P と Q は $K[X]$ の元として互いに素である

[2] P と Q は $K'[X]$ の元として互いに素である

は同値である．

P と Q が互いに素であるとは，その最小公約式が 0 でない定数であるということである．最小公約式を Euclid の互除法で求めることを考えると，P, Q を $K[X]$ の元として考えた場合でも $K'[X]$ の元として考えた場合でも，手続きは同じである．したがって，補題の 2 条件は明らかに同値である．

命題 19. 体 K と多項式 $P \in K[X]$ に対し，

[1] P は分離多項式である
[2] P と P' は互いに素である

は同値である．

P の分解体を K' とする．条件 1 が成り立つとすると，P' は $K'[X]$ において相異なる 1 次式の積に分解する．したがって，$(X-a)^2 \mid P'$ を満たす $a \in K'$ は存在しない．よって補題 17 より，$X-a \mid P$ かつ $X-a \mid P'$ なる $a \in K'$ は存在しない．これは，$a \in K'$ が $X-a \mid P$ を満たせば $X-a \nmid P'$ であることを意味している．すなわち，P の因子を P' は因子としてもたないので，P と P' は $K'[X]$ で互いに素であることになる．これより補題 18 から，P と P' は $K[X]$ でも互いに素になる．したがって，条件 2 が示された．この議論は逆にも辿れるので，2 つの条件の同値性が示された．

命題 20. 体 K と既約多項式 $P \in K[X]$ をとる．このとき，

[1] P は分離多項式ではない
[2] $p := \operatorname{char} K$ とおくと $p > 0$ であり，ある $Q \in K[X]$ が存在して $P = Q(X^p)$ かつ $Q \notin K^p[X]$ が成り立つ

は同値である．

[1]⇒[2]: 条件 1 が成り立つとする．このとき，命題 19 によって P と P' は互いに素ではない．したがって，P と P' の最大公約式 Q は 0 であるか 1 次以上の多項式である．$Q \neq 0$ であるとすると，$Q \mid P$ が成り立つが P は既約なので，Q は P に一致しなければならない．したがって，$Q \mid P'$ より $P \mid P'$ を得るが，微分の定義より $\deg P > \deg P'$ であるからこれは矛盾である．よって $Q = 0$ であり，$P \neq 0$ より $P' = 0$ が分かる．ここで，

$$P =: \sum_{i=0}^{n} a_i X^i \quad (a_i \in K)$$

とおくと，

$$P' = \sum_{i=1}^{n} i a_i X^{i-1}$$

であるから，$P' = 0$ より $ia_i = 0$ $(1 \leq i \leq n)$ が成り立つ．もし $\operatorname{char} K = 0$ であったら，これより $a_i = 0$ $(1 \leq i \leq n)$ となって P は定数になり，既約性に矛盾する．したがって，$\operatorname{char} K > 0$ である．

$p \coloneqq \operatorname{char} K$ とおく．このとき，$p \nmid i$ ならば $a_i = 0$ となる．したがって，

$$Q \coloneqq \sum_{\substack{p|i \\ 0 \le i \le n}} a_i X^{i/p}$$

とおけば，

$$Q(X^p) \coloneqq \sum_{\substack{p|i \\ 0 \le i \le n}} a_i X^i = \sum_{0 \le i \le n} a_i X^i = P$$

が成り立つ．また，もし 1 次以上の多項式 Q_1, Q_2 によって $Q = Q_1 Q_2$ と表すことができるとすると，$P = Q_1(X^p) Q_2(X^p)$ となって P の既約性に矛盾するから，Q は既約である．さらに，もし $Q \in K^p[X]$ であるとすると，

$$Q =: \sum_{i=0}^{m} {b_i}^p X^i \quad (b_i \in K)$$

と表せることになるが，

$$P = Q(X^p) = \sum_{i=0}^{m} {b_i}^p X^{pi} = \left(\sum_{i=0}^{m} b_i X^i \right)^p$$

となって P の既約性に矛盾するから，$Q \notin K^p[X]$ が成り立つ．以上で，条件 2 が示された．

[2]⇒[1]:　条件 2 の $Q \in K[X]$ を

$$Q =: \sum_{i=0}^{n} a_i X^i \quad (a_i \in K)$$

と表す．このとき，

$$P = Q(X^p) = \sum_{i=0}^{n} a_i X^{pi}$$

であるから，$\operatorname{char} K = p$ であることより，

$$P' = \sum_{i=1}^{n} pi a_i X^{pi-1} = 0$$

が成り立つ．よって，P と P' は互いに素とはならないから，命題 19 によって P は分離多項式ではなく，条件 1 が示された．

7.　2016 年 11 月 15 日

7.1.　有限体

定理 21. 有限体の元の個数は必ず素数冪である．

有限体 K を任意にとり，$p \coloneqq \operatorname{char} K$ とおく．$p = 0$ なら，命題 1 によって K は $\mathbb{Q}$ を部分体として含むことになり，K の有限性に矛盾する．したがって $p > 0$ であるから，再び命題 1 によって K は $\mathbb{F}_p$ を含む．$n \coloneqq [K : \mathbb{F}_p]$ とおくと，K の有限性から $n < \infty$ である．これより，K は $\mathbb{F}_p$-線型空間として n 次元であり，$\mathbb{F}_p$ の元の個数は p であるから，K の元の個数は p^n である．

補題 22. 体 K, K' の間の準同型写像 $\sigma, \tau \colon K \to K'$ があるとき，

$$K_0 \coloneqq \{x \in K \mid \sigma(x) = \tau(x)\}$$

は K の部分体である．

体の条件を素直に確かめれば良い．

定理 23. 元の個数が素数冪 $q =: p^n$ となる体は $X^q - X$ の最小分解体となり，それは同型を除いて一意に存在する．

定理 24. 元の個数が素数冪 $q =: p^n$ となる体 K に対し，$\operatorname{Aut}(K)$ は Frobenius 写像で生成される n 次巡回群である．

上の 2 つの定理を同時に示す．

$X^q - X \in \mathbb{F}_p[X]$ の最小分解体を L とする．ここで，

$$(X^q - X)' = qX^{q-1} - 1 = -1 \neq 0$$

であるから，$X^q - X$ と $(X^q - X)'$ は互いに素である．したがって，命題 19 によって $X^q - X$ は分離多項式となるから，これを $L[X]$ の元と見なせば相異なる 1 次式の積に分解する．これにより，$X^q - X$ の根は相異なるから，

$$L_0 \coloneqq \{x \in L \mid x^q - x = 0\}$$

は元の個数が q 個の集合である．

さて，$\operatorname{char} L = \operatorname{char} \mathbb{F}_p = p \neq 0$ であるから，Frobenius 写像 $\varphi \colon L \to L$ が考えられる．このとき，L_0 は

$$L_0 \coloneqq \{x \in L \mid \varphi^n(x) = \mathrm{id}(x)\}$$

と書けるから，補題 22 によってこれは体になる．ところで，最小分解体の定義から，L_0 の全ての元で $\mathbb{F}_p$ 上生成される体が L になるのであった．一方，L_0 はそれ自身が体であることが示されたので，$\mathbb{F}_p(L_0) \subseteq L_0$ である．これによって $L \subseteq L_0$ が分かったので $L = L_0$ である．$\#L = \#L_0 = q$ より，元の個数が q の体が存在することが示された．

元の個数が q の有限体 K を任意にとる．このとき，$\operatorname{char} K = p$ であり，K は $\mathbb{F}_p$ を部分体として含む．

$\sigma \in \mathrm{Aut}(K)$ を任意にとると，$\sigma(1) = 1$ より σ は $\mathbb{F}_p$ の元を変えない [*3]．したがって $\sigma \in \mathrm{Mor}_{\mathbb{F}_p}(K, K)$ である．逆に $\sigma \in \mathrm{Mor}_{\mathbb{F}_p}(K, K)$ をとると，K が有限であることから σ は全単射になるので，$\sigma \in \mathrm{Aut}(K)$ が成り立つ．以上により，$\mathrm{Aut}(K) = \mathrm{Mor}_{\mathbb{F}_p}(K, K)$ である．すると，定理 10 によって，

$$\#\,\mathrm{Aut}(K) = \#\,\mathrm{Mor}_{\mathbb{F}_p}(K, K) \leq [K : \mathbb{F}_p] = n \qquad [\sharp]$$

が成り立つ．

Frobenius 写像 $\varphi\colon K \to K$ を考えると，上の議論によって $\varphi \in \mathrm{Aut}(K)$ であるから，$\langle\varphi\rangle \subseteq \mathrm{Aut}(K)$ が成り立つ．$i = 1, \cdots, n-1$ に対し，

$$K_0 \coloneqq \{x \in K \mid \varphi^i(x) = \mathrm{id}(x)\} = \{x \in K \mid x^{p^i} - x = 0\}$$

とおく．K_0 は p^i 次方程式の根全体の集合だから，その元の個数は p^i 以下である．したがって，$\#K_0 \leq p^i < p^n = q$ より，$K_0 \subsetneq K$ が成り立つ．すなわち $\varphi^i \neq \mathrm{id}$ であるから，$\varphi \in \mathrm{Aut}(K)$ の位数は n 以上である．よって，

$$n \leq \#\langle\varphi\rangle \leq \#\,\mathrm{Aut}(K)$$

が示された．式 $\sharp$ と合わせれば，$\mathrm{Aut}(K) = \langle\varphi\rangle$ であり，φ の位数が n であることが分かる．したがって，$\varphi^n = \mathrm{id}$ となるから，任意の $x \in K$ に対して $x^q - x = 0$ が成り立つ．すなわち，$X^q - X$ は $K[X]$ 上で

$$X^q - X = \prod_{x \in K}(X - x)$$

という 1 次式の積に分解する．すなわち，K は $X^q - X$ の最小分解体である．定理 14 によって最小分解体は全て互いに同型だったので，元の個数が q の体の一意性も示された．

定義 19. 元の個数が素数冪 $q =: p^n$ であるような有限体を $\mathbb{F}_q$ と書く．

元の個数が小さい有限体を調べる．まず，$\mathbb{F}_4$ は $\mathbb{F}_2$ の 2 次拡大である．したがって，$a \in \mathbb{F}_4 \setminus \mathbb{F}_2$ の最小多項式を $P \in \mathbb{F}_2[X]$ とすると，$\mathbb{F}_4 \cong \mathbb{F}_2[X]/\langle P\rangle$ である．この P は 2 次の既約多項式である．$\mathbb{F}_4$ は $X^4 - X$ の最小分解体だから，$\mathbb{F}_4$ の元は全て $X^4 - X$ の根である．したがって，P は $X^4 - X$ をわり切る．一方で，

$$X^2 - X = X(X-1) = \prod_{x \in \mathbb{F}_2}(X - x)$$

であり，P は $\mathbb{F}_2$ に属さない元の最小多項式だから，この $X^2 - X$ とは互いに素である．したがって，

$$P = \frac{X^4 - X}{X^2 - X} = X^2 + X + 1$$

となる．これより，

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle$$

[*3] $\mathrm{Aut}(K)$ は K の自己同型群を表す．

と書ける．

次に，$\mathbb{F}_8$ は $\mathbb{F}_2$ の 3 次拡大である．

$$\prod_{x\in\mathbb{F}_8}(X-x) = X^8 - X = X(X-1)(X^3+X^2+1)(X^3+X+1)$$

であり，X^3+X^2+1 と X^3+X+1 は $\mathbb{F}_2[X]$ でともに既約多項式であるから，

$$\mathbb{F}_8 \cong \mathbb{F}_2[X]/\langle X^3+X^2+1\rangle \cong \mathbb{F}_2[X]/\langle X^3+X+1\rangle$$

となる．

最後に，$\mathbb{F}_9$ は $\mathbb{F}_3$ の 2 次拡大である．したがって，$a \in \mathbb{F}_9 \setminus \mathbb{F}_3$ の最小多項式を $P \in \mathbb{F}_3[X]$ とすれば，これは 2 次の既約多項式である．$\mathbb{F}_3$ 上の 2 次の既約多項式は X^2+1, X^2-X-1, X^2+X-1 の 3 つであることが分かる．実際，

$$\prod_{x\in\mathbb{F}_9}(X-x) = X^9 - X = X(X-1)(X+1)(X^2+1)(X^2-X-1)(X^2+X-1)$$

が成り立っている．これより，

$$\mathbb{F}_9 \cong \mathbb{F}_3[X]/\langle X^2+1\rangle \cong \mathbb{F}_3[X]/\langle X^2 \pm X - 1\rangle$$

である．

7.2. 分離拡大

定義 20. 体の拡大 L/K を考える．$a \in L$ が K 上代数的であり，その最小多項式が分離多項式であるとき，a は K 上**分離的**であるという．また，L が K の代数拡大であり，L の任意の元が K 上分離的であるとき，L は K の**分離拡大**という．

元の個数が素数冪 p^n の有限体 K をとる．任意の元 $a \in K$ の最小多項式を $P \in \mathbb{F}_p[X]$ とすると，P は $X^q - X$ をわり切るが，$X^q - X$ は分離多項式だから P も分離多項式となる．したがって，K は $\mathbb{F}_p$ の分離拡大である．

分離拡大の言葉を用いて，定理 10 に同値な条件をもう 1 つ付け加える．

定理 25. 体 K とその拡大体 L, K' をとり，L は K の有限次拡大とする．このとき，

$$\#\mathrm{Mor}_K(L,\, K') \le [L:K] \qquad [\heartsuit]$$

が成り立ち，

[1] 式 ♡ が等号で成り立つ

[2] L の任意の元の K 上最小多項式は，K' 上で相異なる 1 次式の積に分解する

[3] ある $x_1, \cdots, x_n \in L$ が存在して，$L = K(x_1, \cdots, x_n)$ が成り立ち，x_1, $\cdots$, x_n の各 K 上最小多項式が K' 上で相異なる 1 次式の積に分解する

[4] L は K の分離拡大で，L の任意の元の共役は全て K' に属する

は同値である．

定理 10 において，最初の主張と条件 1, 2, 3 の同値性はすでに示されている．したがって，条件 2 と条件 4 の同値性を示せば十分であるが，これは単に言葉を言い換えたに過ぎない．

命題 26. 体 K とその有限次拡大 L に対し，

[1] L は K の分離拡大である

[2] K 上分離的な元 $a_1, \cdots, a_n \in L$ であって $L = K(a_1, \cdots, a_n)$ となるものが存在する

[3] K の拡大体 K' が L の任意の元の K 上の共役を全て属するなら，

$$\#\mathrm{Mor}_K(L, K') = [L : K]$$

を満たす

は同値である．

[1]⇒[2]: L は有限次拡大だから，$L = K(a_1, \cdots, a_n)$ を満たすような $a_1, \cdots, a_n \in L$ はとれる．条件 1 から L は分離拡大なので，$a_1, \cdots, a_n$ は分離的である．

[2]⇒[3]: 条件 2 の $a_1, \cdots, a_n \in L$ をとり，それぞれの最小多項式を $P_1, \cdots, P_n \in K[X]$ とする．$P_1 \cdots P_n$ の分解体を K' とすれば，命題 15 によって K' は L の任意の元の共役を全て属するので，定理 25 の条件 3 と条件 1 の同値性により，示された．

[3]⇒[1]: 定理 25 の条件 1 と条件 4 の同値性から明らかである．

命題 27. 体 K とその有限次拡大 L をとり，拡大 L/K の中間体 M をとる．このとき，

[1] L は K の分離拡大である

[2] M は K の分離拡大で，L は M の分離拡大である

は同値である．

L は K の分離拡大であれば，明らかに M は K の分離拡大である．したがって，M/K が分離的であるという仮定のもとで，L/K が分離的であることと L/M が分離的であることの同値性を示せば良い．

L/K が分離的であるとする．任意の $a \in L$ に対し，その K 上最小多項式を $P \in K[X]$ とし，M 上最小多項式を $Q \in M[X]$ とする．仮定から P は分離多項式である．一方で Q は P をわり切るから，Q も分離多項式である．以上により，L/M は分離的である．

逆に L/M が分離的であるとする．

命題 28. 体 K とその有限次分離拡大 L_1, L_2 をとる．このとき，合成体 $L_1 \cdot L_2$ は K の分離拡大である．

命題 26 により，K 上分離的な元 $a_1, \cdots, a_m, b_1, \cdots, b_n \in L$ が存在して，$L_1 = K(a_1, \cdots, a_m)$ および

$L_2 = K(b_1, \cdots, b_n)$ が成り立つ．このとき，$L_1 \cdot L_2 = K(a_1, \cdots, a_m, b_1, \cdots, b_n)$ であるから，再び命題 26 によって $L_1 \cdot L_2$ は K の分離拡大である．

命題 29. 体 K とその拡大体 L に対し，

$$L_{\mathrm{s}} \coloneqq \{a \in L \mid a \text{ は } K \text{ 上分離的 }\}$$

は L の部分体である．

任意に $a, b \in L_{\mathrm{s}}$ をとると，$K(a)$, $K(b)$ は K の分離拡大である．したがって，命題 28 によって，その合成体 $K(a, b)$ も K の分離拡大である．$a + b$, ab, a^{-1} は全て $K(a, b)$ に属するから，これらは K 上分離的であり L_{s} に属する．

定義 21. 体 K とその拡大体 L に対し，L の部分体

$$L_{\mathrm{s}} \coloneqq \{a \in L \mid a \text{ は } K \text{ 上分離的 }\}$$

を L における K の**分離閉包**という．

命題 30. 体 K をとり，$p \coloneqq \operatorname{char} K$ とおく．このとき，

[1] K の任意の代数拡大は分離拡大である

[2] $p = 0$ であるか，$p > 0$ であって $K^p = K$ が成り立つ

は同値である．

[1]⇒[2]: 条件 2 が成り立たないとすると，$p > 0$ であり $K^p \neq K$ である．したがって，$a \in K \setminus K^p$ が存在する．

$X^p - a \in K[X]$ を考え，この分解体を K' とする．$X^p - a$ は $K'[X]$ においては 1 次式の積に分解するから，この根 $b \in K'$ が存在する．すなわち $b^p = a$ が成り立つ．したがって，p 乗写像が体の準同型写像になることに注意して，

$$X^p - a = X^p - b^p = (X - b)^p$$

が成り立つ．ここで，$X^p - a$ が $K[X]$ において既約でないとすると，定数でないモニック多項式 $P, Q \in K[X]$ が存在して $PQ = X^p - a$ と表せる．したがって，$K'[X]$ において $PQ = (X - b)^p$ が成り立つから，ある $P = (X - b)^i$ $(0 < i < p)$ となる．これの $i - 1$ 次の項の係数は $-ib$ であるから，$P \in K[X]$ より $ib \in K$ となる．$0 < i < p$ より K の元として $i \neq 0$ だから，$b \in K$ を得る．これにより，$a = b^p \in K^p$ となるが，これは矛盾である．以上により，$X^p - a \in K[X]$ は既約である．

これによって，$L \coloneqq K[X]/\langle X^p - a\rangle$ は K の代数拡大になる．$\overline{X} \in L$ の最小多項式は $X^p - a$ となるが，これは分離多項式ではないので，L は K の分離拡大ではない．したがって，条件 1 の否定が示された．この対偶をとれば，条件 1 から条件 2 が導かれる．

[2]⇒[1]: 条件 1 が成り立たないとする．このとき，分離的でない既約多項式 $P \in K[X]$ が存在する．

命題 20 によって，まず $p > 0$ であり，$Q \in K[X] \setminus K^p[X]$ が存在するから，特に $K \neq K^p$ である．したがって，条件 2 の否定が示された．対偶をとれば，条件 2 から条件 1 が導かれる．

定義 22. 体 K が命題 30 の同値な条件を満たすとき，K を**完全体**という．

標数が 0 の体は全て完全体だから，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は完全体である．また，有限体 $\mathbb{F}_q$ に対して Frobenius 写像が全単射になるので，$\mathbb{F}_q$ は完全体である．一方，標数が正の体 K に対して，その有理関数体 $K(X)$ は完全体にはならない．実際，$X \in K(X)$ であるが $X \notin K(X)^p$ である．

8. 2016 年 11 月 22 日

8.1. 分離拡大の中間体

有限次分離拡大 L/K があるとし，K の拡大体 K' が L の任意の元の K 上の共役を全て属するとする．$S := \mathrm{Mor}_K(L, K')$ とおくと，命題 26 によって $\#S = [L : K]$ である．もし $a \in L$ によって $L = K(a)$ と書けるなら，補題 9 によって，a の最小多項式の K' 上の根の個数が $\#S$ に一致するのだった．

さて，この有限次分離拡大 L/K の中間体 M について調べたい．$S_M := \mathrm{Mor}_K(M, K')$ とすれば，命題 16 によって，$\sigma \in S$ を $\sigma|_M \in S_M$ に移す写像は全射であった．したがって，S 上の関係 $\sim_M$ を，

$$\sigma \sim_M \tau :\Longleftrightarrow \sigma|_M = \tau|_M$$

によって定義すれば，これは同値関係となり，$S/\sim_M$ と S_M の間には 1 対 1 の対応ができる．また，

$$\mathscr{M} := \{M \mid M \text{ は } L/K \text{ の中間体 }\}$$
$$\mathscr{E} := \{\sim \mid \sim \text{ は } S \text{ 上の同値関係 }\}$$

とおくと，上記の記号を用いて写像

$$\Sigma\colon\ \mathscr{M} \to \mathscr{E};\ M \mapsto \sim_M$$

が定義でき，これによって L/K の中間体と S の同値関係が結びつく．なお，次に示すように Σ は単射になる．また，L/K が後に定義する Galois 拡大になっていれば，Σ の像を記述できることが分かる．

命題 31. 有限次分離拡大 L/K の中間体 M に対し，

$$M = \{x \in L \mid \sigma \sim_M \tau \text{ ならば } \sigma(x) = \tau(x)\}$$

が成り立つ．

命題の式の右辺を M' とおくと，これも L/K の中間体である．$\sim_M$ の定義から $M \subseteq M'$ は明らかに成り立つので，これの逆の包含関係を示せば良い．

$\sigma \sim_M \tau$ が成り立っているとすると，M' の定義から，任意の $x \in M'$ に対して $\sigma(x) = \tau(x)$ が成り立

つ．すなわち $\sigma|_{M'} = \tau|_{M'}$ が成り立つので，$\sigma \sim_{M'} \tau$ である．以上により，$\sim_M \subseteq \sim_{M'}$ である [*4]．これにより，

$$\dim_K M = [M : K] = \#S_M = \#(S/\sim_M) \leq \#(S/\sim_{M'}) = \dim_K M'$$

を得るが，$M \subseteq M'$ より上式の不等号は等号でなければならないので，$M = M'$ となる．

命題 32. 有限次分離拡大 L/K の中間体 M, M' に対し，

[1] $M \subseteq M'$ が成り立つ

[2] $\sim_M \supseteq \sim_{M'}$ が成り立つ

は同値である．

[1]⇒[2]: 定義から自明である．

[2]⇒[1]: 条件 2 から，

$$\{x \in L \mid \sigma \sim_M \tau \text{ ならば } \sigma(x) = \tau(x)\} \subseteq \{x \in L \mid \sigma \sim_{M'} \tau \text{ ならば } \sigma(x) = \tau(x)\}$$

が分かるが，命題 31 よりこの右辺は M と一致し左辺は M' と一致する．

命題 33. 有限次分離拡大 L/K について，K の拡大体 K' が L の任意の元の共役を全て属するとする．このとき，$a \in L$ について，

[1] $L = K(a)$ が成り立つ

[2] $\sigma \in \mathrm{Mor}_K(L, K')$ を $\sigma(a) \in K'$ に移す写像は単射である

は同値である．また，上記の同値な条件を満たす $a \in L$ は常に存在する．

条件 1 は $\sim_{K(a)} = \sim_L$ と同値である．ここで，$\sigma \sim_{K(a)} \tau$ は，σ, τ が K の元を変えないことに注意して，$\sigma(a) = \tau(a)$ と同じ意味である．一方，$\sigma \sim_L \tau$ は常に成り立つ．したがって，$\sim_{K(a)} = \sim_L$ が成り立つことは，$\sigma(a) = \tau(a)$ なら $\sigma = \tau$ であることと同値である．これは条件 2 の写像が単射ということである．

さて，上記の条件 2 を満たす $a \in L$ の存在を示す．条件 2 の写像が単射であるためには，

$$a \notin \bigcup_{\substack{\sigma,\tau \in \mathrm{Mor}_K(L,K') \\ \sigma \neq \tau}} \{x \in L \mid \sigma(x) = \tau(x)\} \qquad [\sharp]$$

であれば良いから，これを満たすような $a \in L$ を見つける．

K が無限体であるとする．上式の右辺にある $\{x \in L \mid \sigma(x) = \tau(x)\}$ は L/K の部分体であって L には一致しない．したがって，これは K-線型空間として L の真の部分空間である．K-線型空間は，その真の部分空間の有限個の合併では書けないことが知られているから，式 $\sharp$ のような $a \in L$ は必ず存在する．

[*4] ここで，S 上の同値関係を $S \times S$ の部分集合と同一視している．すなわち，この同一視のもとでは，$\sigma \sim \tau$ が成り立つとは $(\sigma, \tau) \in \sim \subseteq S \times S$ と同じ意味になる．以降も同様の同一視を行う．

次に，K が有限体である場合を考える．$p \coloneqq \mathrm{char}\, K$ とする．L は K の有限次拡大であるから L も有限体となるので，$L = \mathbb{F}_{p^n}$ と見なして良い．このとき，$\mathbb{F}_p \subseteq K \subseteq L = \mathbb{F}_{p^n}$ なので，$\mathbb{F}_{p^n} = \mathbb{F}_p(a)$ となる $a \in \mathbb{F}_{p^n}$ を見つければ良い．

さて，任意に $x \in \mathbb{F}_{p^n}$ をとると $x^q - x = 0$ だから，x の $\mathbb{F}_p$ 上最小多項式は $X^q - X$ をわり切る．$\mathbb{F}_{p^n}$ は $X^q - X$ の最小分解体だったから，P の分解体でもある．すなわち，$\mathbb{F}_{p^n}$ は $\mathbb{F}_{p^n}$ の任意の元の $\mathbb{F}_p$ 上共役を全て属する．以上によって，$K = \mathbb{F}_p$, $L = \mathbb{F}_{p^n}$, $K' = \mathbb{F}_{p^n}$ としたときの式 ♯ を満たす $a \in \mathbb{F}_{p^n}$ を見つければ十分である． Frobenius 写像を $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ とおくと，定理 24 によって $\mathrm{Aut}(\mathbb{F}_{p^n})$ は φ を生成元とする n 次巡回群である．したがって，任意の $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_{p^n})$ について $\sigma = \varphi^i$, $\tau = \varphi^j$ $(0 \leq i, j < n)$ と表せる．このとき，

$$\{x \in \mathbb{F}_{p^n} \mid \sigma(x) = \tau(x)\} = \{x \in \mathbb{F}_{p^n} \mid \varphi^{i-j}(x) = x\}$$

と書ける．σ, τ が $\mathrm{Aut}(\mathbb{F}_{p^n})$ の相異なる元を動くとき，$j - i$ は 1 以上 n 未満の整数を動くから，式 ♯ の右辺は

$$T \coloneqq \bigcup_{l=1}^{n-1} \{x \in \mathbb{F}_{p^n} \mid \varphi^l(x) = x\} = \bigcup_{l=1}^{n-1} \{x \in \mathbb{F}_{p^n} \mid x^{p^l} - x = 0\}$$

に等しい．ここで，$x^{p^l} - x = 0$ を満たす $x \in \mathbb{F}_{p^n}$ は高々 p^l 個しかないので，

$$\#T \leq \sum_{l=1}^{n-1} p^l = \frac{p^n - p}{p - 1} < p^n = \#\mathbb{F}_{p^n}$$

が成り立つ．したがって，T は $\mathbb{F}_{p^n}$ とは一致しないから，$a \in \mathbb{F}_{p^n} \setminus T$ が存在し，これが求めるものであった．

9. 2016 年 12 月 6 日

9.1. 正規拡大

定義 23. 代数拡大 L/K に対し，L が L 自身の任意の元の共役を全て属するとき，L/K を**正規拡大**という．

命題 34. 有限次拡大 L/K とその中間体 M について，L は M の任意の元の K 上共役を全て属するとする．このとき，

[1] M/K は正規拡大である

[2] 任意の $\varphi \in \mathrm{Mor}_K(M, L)$ に対して $\varphi(M) \subseteq M$ が成り立つ

は同値である．

[1]⇒[2]: 任意に $\varphi \in \mathrm{Mor}_K(M, L)$ をとる．M/K は正規拡大なので，M は M の任意の元の K 上共役を全て属する．したがって，命題 15 の条件 1 と条件 3 の同値性により，$\varphi(M) \subseteq M$ が成り立つ．よって，条件 2 が示された．

[2]⇒[1]: $L' \coloneqq L \cdot K'$ とおき，$L \subseteq L'$ および $K' \subseteq L'$ と見る．任意に K-準同型写像 $\varphi\colon M \to K'$ をとると，これは $\varphi\colon M \to L'$ と見ることができる．L は M の任意の元の共役を全て属するので，命題 15 によって $\varphi(M) \subseteq L$ を満たす．これにより，$\varphi\colon M \to L$ と見なすことができ，条件 2 によって $\varphi(M) \subseteq M$ が成り立つ．これは，命題 15 を再び使うことで，M が M の任意の元の共役を全て属することを意味する．すなわち，M は K の正規拡大であり，条件 1 が示された．

命題 35. 体 K とその有限次正規拡大 L_1, L_2 をとる．このとき，合成体 $L_1 \cdot L_2$ は K の正規拡大である．

命題 15 の条件 1 と条件 2 の同値性を使えば明らかである．

9.2. Galois 拡大

定義 24. 拡大 L/K に対し，

$$\mathrm{Aut}_K(L) \coloneqq \{\varphi\colon L \to L \mid \varphi \text{ は } K \text{ 上の体の同型写像 }\}$$

と書く．

定義から明らかに $\mathrm{Aut}_K(L) \subseteq \mathrm{Mor}_K(L, L)$ である．L/K が有限次拡大であれば，$\varphi \in \mathrm{Aut}_K(L)$ は同じ有限次元 K-線型空間の間の単射 K-線型写像であるから，同型写像になる．すなわち，このときは $\mathrm{Aut}_K(L) = \mathrm{Mor}_K(L, L)$ が成り立つ．

定義 25. 有限次拡大 L/K に対し，$\#\mathrm{Aut}_K(L) = [L : K]$ を満たすとき L/K を **Galois 拡大**という．また，$\mathrm{Gal}(L/K) \coloneqq \mathrm{Aut}_K(L)$ を L/K の **Galois 群**という．

$\mathbb{C}$ 上の体の自己同型写像で $\mathbb{R}$ の元を動かさないものは，恒等写像と共役写像のみである．したがって $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = 2$ であり，一方で $[\mathbb{C} : \mathbb{R}] = 2$ であるから，拡大 $\mathbb{C}/\mathbb{R}$ は Galois 拡大である．また，$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ である．

素数冪 p^n に対し，定理 24 によって $\mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_p)$ は n 次巡回群であったから，特に $\#\mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_p) = n$ である．一方で $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ だから，拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ は Galois 拡大であり $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ である．

拡大 L/K が Galois 拡大であり，ある $a \in L$ によって $L = K(a)$ と表せたとする．このとき，a の最小多項式を $P \in K[X]$ とすれば，$L \cong K[X]/\langle P\rangle$ である．ここで，

$$S \coloneqq \{x \in L \mid P(x) = 0\}$$
$$T \coloneqq \mathrm{Mor}_K(L, L) = \mathrm{Aut}_K(L)$$

とおくと，補題 9 により S と T の間に 1 対 1 対応があるのであった．$n \coloneqq [L : K]$ とおけば，Galois 拡大の定義から $\#T = n$ である．したがって $\#S = n$ でもあるが，P の次数は n なので，P は $L[X]$ で

相異なる 1 次式の積に分解しなければならない．この分解を，

$$P =: \prod_{i=1}^{n}(X - a_i) \quad (a_i \in L)$$

とおく．ところで，上の S と T の対応は，$\sigma \in T$ に対し $\sigma(a) \in S$ を対応させるというものであった．したがって，$S =: \{\sigma_1, \cdots, \sigma_n\}$ とおけば，添字の順番を適宜入れ替えることで，$a_i = \sigma_i(a)$ と表せる．よって P の分解は，

$$P = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(a))$$

と書ける．すなわち，Galois 群によって P の 1 次式の積への分解が得られ，P の 1 次式への分解から Galois 群も決まるのである．

命題 36. 有限次拡大 L/K に対し，

[1] L/K は Galois 拡大である

[2] L/K は分離拡大かつ正規拡大である

は同値である．

この命題の主張は，定理 25 の条件 1 と条件 4 の同値性そのものである．

命題 37. 体 K とその有限次 Galois 拡大 L_1, L_2 をとる．このとき，合成体 $L_1 \cdot L_2$ は K の Galois 拡大である．

命題 28, 35, 36 を合わせれば明らかである．

さて，命題 36 により Galois 拡大では分離拡大であることが分かる．ただし，全ての分離拡大が Galois 拡大になるとは限らない．しかし，以下のようにして，分離拡大を含むような Galois 拡大を構成することはできる．

有限次分離拡大 L/K と K の拡大体 K' に対し，K' は L の任意の元の K 上共役を全て属するとする．$n \coloneqq [L : K]$ とおけば，定理 25 によって $\#\mathrm{Mor}_K(L, K') = n$ である．そこで，$\mathrm{Mor}_K(L, K')$ の相異なる元を $\sigma_1, \cdots, \sigma_n$ とすれば，$\sigma_1(L), \cdots, \sigma_n(L)$ は K' の部分体であるから，これら全ての合成体 $\tilde{L} \leq K'$ をとることができる．

命題 38. 有限次分離拡大 L/K と K の拡大体 K' に対し，K' は L の任意の元の K 上共役を全て属するとする．上記の $\tilde{L}$ に対し，拡大 $\tilde{L}/K$ は有限次 Galois 拡大である．

各 $\sigma_i(L)$ は L と同型であるから K の有限次拡大になっている．したがって，それらの合成体である $\tilde{L}$ も K の有限次拡大である．同じように，各 $\sigma_i(L)$ は K の分離拡大でもあるので，命題 28 によって $\tilde{L}$ も K の分離拡大である．

$\sigma_i(L)$ たちの K 上生成元を全て集めれば $\tilde{L}$ の K 上生成元になる．K' はこれらの生成元の共役は全て属するので，定理 25 の条件 2 と条件 3 の同値性を使うことで，K' は $\tilde{L}$ の任意の元の共役を全て属

することが分かる．ところで，任意の $\varphi \in \mathrm{Mor}_K(\tilde{L}, K')$ に対し，

$$\begin{aligned}\varphi(\tilde{L}) &= \varphi(\sigma_1(L) \cdot \cdots \cdot \sigma_n(L)) \\ &= \varphi(\sigma_1(L)) \cdot \cdots \cdot \varphi(\sigma_n(L))\end{aligned}$$

が成り立つ．$\varphi \circ \sigma_i \in \mathrm{Mor}_K(L, K')$ であるから，$\tilde{L}$ の定義から上式の最右辺は $\tilde{L}$ に含まれる．したがって $\varphi(\tilde{L}) \subseteq \tilde{L}$ が示された．これにより，$\tilde{L}$ は $\tilde{L}$ の任意の元の共役を全て属するから，命題 34 によって $\tilde{L}$ は K の正規拡大である．

以上により，命題 36 によって $\tilde{L}/K$ は有限次 Galois 拡大である．

定義 26. 有限次分離拡大 L/K に対し，上記の $\tilde{L}$ を L の **Galois 閉包**という．

Galois 拡大の中間体と自己同型群の部分群の対応を調べる．

定義 27. 拡大 L/K と有限部分群 $G \leq \mathrm{Aut}_K(L)$ に対し，

$$L^G \coloneqq \{x \in L \mid \text{任意の } \sigma \in G \text{ に対し } \sigma(x) = x\}$$

を G における**不変部分体**という．

不変部分体が実際に体になることは補題 22 から従う．これは拡大 L/K の中間体になっている．

定理 39. 拡大 L/K と有限部分群 $G \leq \mathrm{Aut}_K(L)$ に対し，

[1] L/K は有限次 Galois 拡大であり，G はその Galois 群である
[2] $K = L^G$ が成り立つ

は同値である．

[1]⇒[2]: L/K は有限次 Galois 拡大なので，命題 36 により L/K は有限次分離拡大でもある．G は Galois 群だから，$G = \mathrm{Mor}_K(L, L)$ である．命題 31 を使えば，

$$\begin{aligned}K &= \{x \in L \mid \text{任意の } \sigma, \tau \in \mathrm{Mor}_K(L, L) \text{ に対し } \sigma \sim_K \tau \text{ ならば } \sigma(x) = \tau(x)\} \\ &= \{x \in L \mid \text{任意の } \sigma, \tau \in G \text{ に対し } \sigma(x) = \tau(x)\} \\ &= \{x \in L \mid \text{任意の } \sigma' \in G \text{ に対し } \sigma'(x) = x\} \\ &= L^G\end{aligned}$$

が分かる．

[2]⇒[1]: $L' \coloneqq \bigoplus_{\sigma \in G} L$ とおき，これを L-線型空間と見なす．また，L を K-線型空間を見なす．写像

$$F\colon\ L \to L';\ y \mapsto (\sigma(y))_{\sigma \in G}$$

は K-線型写像であり，各 $\sigma \in G$ が単射であることから Φ も単射である．

$y_1, \cdots, y_m \in L$ が K 上線型独立ならば $F(y_1), \cdots, F(y_m) \in L'$ が L 上線型独立であることを示す．m に関する帰納法による．$m = 1$ ならば，示すべきことはない．$m \geq 2$ とする．$F(y_1), \cdots, F(y_m)$ が線

型独立でないとすると，ある $a_i \in L$ たちによって，

$$F(y_m) = \sum_{i=1}^{m-1} a_i F(y_i)$$

と書ける．F の定義から，これは任意の $\sigma \in G$ に対し，

$$\sigma(y_m) = \sum_{i=1}^{m-1} a_i \sigma(y_i)$$

が成り立つことを意味する．したがって，さらに任意の $\tau \in G$ に対し，

$$\tau(\sigma(y_m)) = \sum_{i=1}^{m-1} \tau(a_i)\tau(\sigma(y_i))$$

が成り立つ．ここで，$\sigma' \coloneqq \tau \circ \sigma$ とおくと，

$$\sigma'(y_m) = \sum_{i=1}^{m-1} \tau(a_i)\sigma'(y_i)$$

となるが，σ が G 全体を動くとき σ' も G 全体を動くから，これは

$$F(y_m) = \sum_{i=1}^{m-1} \tau(a_i) F(y_i)$$

を意味する．最初の式と比べれば，

$$\sum_{i=1}^{m-1} a_i F(y_i) = \sum_{i=1}^{m-1} \tau(a_i) F(y_i)$$

を得るが，帰納法の仮定から $F(y_1), \cdots, F(y_{m-1})$ は線型独立なので，$a_i = \tau(a_i)$ を得る．$\tau \in G$ は任意にとれたので，$a_i \in L^G = K$ を得る．すると，$F(a_i) = a_i$ だから，

$$F(y_m) = \sum_{i=1}^{m-1} F(a_i y_i)$$

となり，F が単射であることから，

$$y_m = \sum_{i=1}^{m-1} a_i y_i$$

を得るが，これは $y_1, \cdots, y_m$ が線型独立であることに矛盾する．以上で主張は示された．

さて，これより L において K 上線型独立な元が $\dim_L L'$ 個より多くとれたとすると，それらの F の像は L' において L 上線型独立であるが，それは矛盾である．したがって，L における K 上線型独立な元は高々 $\dim_L L'$ 個しかとれない．これより $\dim_K L \leq \dim_L L'$ が得られ，さらに

$$[L : K] = \dim_K L \leq \dim_L L' = \#G \leq \#\operatorname{Aut}_K(L) = \#\operatorname{Mor}_K(L, L) \leq [L : K]$$

が分かる．この最両辺は一致しているので，ここに出てくる不等号は全て等号でなければならない．$\#\operatorname{Aut}_K(L) = [L : K]$ であるから L/K は Galois 拡大であり，$G = \operatorname{Aut}_K(L)$ より G はその Galois 群である．

定理 40.［Galois 理論の基本定理］ 有限次 Galois 拡大 L/K をとり，$G := \mathrm{Gal}(L/K)$ とおく．L/K の中間体 M に対し，L/M は有限次 Galois 拡大であり，$H := \mathrm{Gal}(L/M)$ とおくと $M = L^H$ が成り立つ．逆に，G の部分群 H に対し，$M := L^H$ とおくと L/M は有限次 Galois 拡大で，$H = \mathrm{Gal}(L/M)$ が成り立つ．

L/K の中間体 M をとる．L/M は明らかに有限次拡大である．L/K は分離拡大なので，命題 27 より L/M も分離拡大である．また，L/K は正規拡大なので，正規拡大の定義から明らかに L/M も正規拡大である．したがって，L/M は有限次 Galois 拡大である．また，定理 39 により，$M = L^H$ である．

逆に，G の部分群 H をとる．定理 39 により，L/M は有限次分離拡大であって H はその Galois 群である．

定理 40 の主張は次のように言い換えることができる．すなわち，有限次 Galois 拡大 L/K に対し，

$$\mathscr{M} := \{M \mid M \text{ は } L/K \text{ の中間体 }\}$$
$$\mathscr{H} := \{H \mid H \text{ は } \mathrm{Gal}(L/K) \text{ の部分群 }\}$$

とおくと，

$$\Phi\colon\ \mathscr{M} \to \mathscr{H};\ M \mapsto \mathrm{Gal}(L/M)$$
$$\Psi\colon\ \mathscr{H} \to \mathscr{M};\ H \mapsto L^H$$

は互いに逆写像である．

命題 41. 有限次 Galois 拡大 L/K とその中間体 M, M' をとる．M, M' に対応する群をそれぞれ H, H' とすると，

[1] $M \subseteq M'$ が成り立つ

[2] $H \supseteq H'$ が成り立つ

は同値である．

中間体と群の対応から明らかである．

命題 42. 有限次 Galois 拡大 L/K をとり，$G := \mathrm{Gal}(L/K)$ とする．L/K の中間体 M に対応する群を H とするとき，$\sigma \in G$ に対して $\sigma(M)$ に対応する群は $\sigma H \sigma^{-1}$ である．

$\sigma(M)$ に対応する群を H' とすると，$H' = \mathrm{Gal}(L/\sigma(M))$ なので，

$$\begin{aligned} H' &= \{\tau \in G \mid x \in \sigma(M) \text{ ならば } \tau(x) = x\} \\ &= \{\tau \in G \mid y \in M \text{ ならば } \tau(\sigma(y)) = \sigma(y)\} \\ &= \{\tau \in G \mid y \in M \text{ ならば } (\sigma^{-1}\tau\sigma)(y) = y\} \\ &= \{\tau \in G \mid \sigma^{-1}\tau\sigma \in H\} \\ &= \sigma H \sigma^{-1} \end{aligned}$$

が成り立つ．

命題 43. 有限次 Galois 拡大 L/K をとり，$G := \mathrm{Gal}(L/K)$ とする．L/K の中間体 M に対応する群を H とするとき，

[1] 拡大 M/K は Galois 拡大である

[2] H は G の正規部分群である

は同値である．また，このとき $\mathrm{Gal}(M/K) \cong G/H$ が成り立つ．

L/K は特に分離拡大なので，命題 27 より M/K は分離拡大である．したがって，M/K が正規拡大であることと H が G の正規部分群であることの同値性を示せば良い．

L/K は正規拡大なので，L は M の任意の元の共役を全て属する．したがって，命題 34 により，M/K が正規拡大であることは，任意の $\sigma \in \mathrm{Mor}_K(M, L)$ に対して $\sigma(M) \subseteq M$ が成り立つことと同値である．L/K は正規拡大なので，L は L の任意の元の共役を全て属するから，命題 16 により，

$$R\colon\ \mathrm{Mor}_K(L, L) \to \mathrm{Mor}_K(M, L);\ \tau \mapsto \tau|_M$$

は全射である．すなわち，ある $\tau \in \mathrm{Mor}_K(L, L)$ によって $\tau|_M = \sigma$ と書ける．これより，任意の $\tau \in G$ に対して $\tau(M) \subseteq M$ が成り立つ．τ は単射なので $\tau(M)$ と M は同型だから，$\tau(M) \subseteq M$ より $\tau(M) = M$ である．Galois 群との対応を考えれば，M は H と対応し，命題 42 によって $\tau(M)$ は $\tau H \tau^{-1}$ と対応するので，$H = \tau H \tau^{-1}$ が成り立つ．これが任意の $\tau \in G$ について成り立つので，これはつまり H が G の正規部分群ということである．この議論は逆にも辿れるので，同値性が示された．

また，命題の同値な 2 条件が成り立つとする．写像

$$\Phi\colon\ \mathrm{Mor}_K(M, M) \to \mathrm{Mor}_K(M, L);\ \sigma \mapsto \sigma$$

は単射である．また，上の議論によって任意の $\sigma \in \mathrm{Mor}_K(M, L)$ は $\sigma(M) \subseteq M$ を満たすから，$\sigma \in \mathrm{Mor}_K(M, M)$ と見なせる．すなわち，Φ は全射である．したがって，$\Psi := \Phi^{-1} \circ R$ とおくと，写像 $\Psi\colon G \to \mathrm{Gal}(M/K)$ が定まる．Ψ は明らかに群準同型写像になっており，R が全射であることから Ψ も全射である．ここで，

$$\mathrm{Ker}\,\Psi = \{\sigma \in G \mid \sigma|_M = \mathrm{id}_M\} = \mathrm{Mor}_M(L, L) = H$$

であるから，準同型定理により $\mathrm{Gal}(M/K) \cong G/H$ である．

命題 44. 有限次 Galois 拡大 L/K をとり，$G := \mathrm{Gal}(L/K)$ とおく．また，K の拡大体 K' をとる．$L' := L \cdot K'$ を K 上の合成体とすると，拡大 L'/K' は有限次 Galois 拡大で $G' := \mathrm{Gal}(L'/K')$ とおくと，群準同型写像

$$\Phi\colon\ G' \to G;\ \sigma \mapsto \sigma|_L$$

が定義されて単射である．さらに，$\mathrm{Im}\,\Phi$ は $L \cap K'$ と対応する G の部分群である．

L' 内で $L' = K'(L)$ と書けるから，L'/K' が有限次分離拡大なのは自明である．L/K は有限次拡大より，$L = K(a_1, \cdots, a_n)$ と書け，$L' = K'(a_1, \cdots, a_n)$ と表せる．各 $a_i \in L$ の K 上最小多項式を

$P_i \in K[X]$ とすれば，P_i は $L[X]$ で 1 次式の積に分解するので，$L'[X]$ でも 1 次式の積に分解する．$P_i \in K'[X]$ と見なせて $P_i(a_i) = 0$ だから，命題 15 の条件 2 と条件 1 の同値性により，L' は L' の K' 上共役を全て属する．これによって L'/K' は正規拡大なので，上の結果と合わせて L'/K' は有限次 Galois 拡大である．

任意に $\sigma \in G'$ をとると，$\sigma|_L : L \to L'$ は K-準同型写像である．L が L の K 上共役を全て属すので，命題 15 から $\sigma(L) \subseteq L$ が成り立つ．しかし，$\sigma(L) \cong L$ なので，$\sigma(L) = L$ である．すなわち，$\sigma|_L : L \to L$ は同型写像であるから，$\sigma|_L \in G$ である．これにより，Φ は矛盾なく定義でき，明らかに群準同型写像である．

$\sigma \in \operatorname{Ker}\Phi$ を任意にとると $\sigma|_L = \mathrm{id}_L$ である．$\sigma \in G' = \operatorname{Mor}_{K'}(L', L')$ だから $\sigma|_{K'} = \mathrm{id}_{K'}$ でもある．$L' = L \cdot K'$ なので，これより $\sigma = \mathrm{id}_{L'}$ を得る．すなわち，Φ は単射である．また，$\operatorname{Im}\Phi$ に対応する中間体を M とおけば，

$$\begin{aligned} M &= \{x \in L \mid \sigma \in \operatorname{Im}\Phi \text{ ならば } \sigma(x) = x\} \\ &= \{x \in L \mid \tau \in G' \text{ ならば } \tau(x) = x\} \end{aligned}$$

であるが，$G' = \operatorname{Gal}(L'/K')$ より，

$$K' = \{x \in L' \mid \tau \in G' \text{ ならば } \tau(x) = x\}$$

であったから，上の式と見比べて $M = L \cap K'$ である．

定義 28. Galois 拡大 L/K に対し，$\operatorname{Gal}(L/K)$ が Abel 群であるとき L/K を **Abel 拡大**という．

素数冪 p^n に対し，拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ を考える．これは有限次 Galois 拡大で，$\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ となり，その生成元は Frobenius 写像である．ここで，$\mathbb{Z}/n\mathbb{Z}$ の部分群と n の正の約数は 1 対 1 に対応していることから，$\mathbb{F}_{p^n}/\mathbb{F}_p$ の中間体がちょうど n の正の約数の個数分だけあることが分かる．

$d \mid n$ なる正整数 d をとり，$m := n/d$ とする．$m\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$ より，$m\mathbb{Z}/n\mathbb{Z}$ に対応する中間体 M がある．命題 43 により，

$$\operatorname{Gal}(M/\mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

であるから，

$$[M : \mathbb{F}_p] = \#\operatorname{Mor}_{\mathbb{F}_p}(M, M) = \#\operatorname{Gal}(M/\mathbb{F}_p) = \#(\mathbb{Z}/m\mathbb{Z}) = m$$

が分かる．すなわち，M は $\mathbb{F}_p$ の m 次拡大だから $\mathbb{F}_{p^m}$ である．

体 k をとり，n 変数有理関数体 $L := k(X_1, \cdots, X_n)$ を考える．G を n 次対称群とすると，変数の添字の置換として G は L に作用する．すると，定理 40 によって $\operatorname{Gal}(L/L^G) = G$ である．この L^G を具体的に求めたい．

T を不定元とする多項式

$$P_n := \prod_{i=1}^{n} (T - X_i) \in L[T]$$

の i 次の項の係数を $S_i \in L$ とする．具体的には，

$$\begin{aligned} S_1 &= X_1 + X_2 + \cdots + X_n \\ S_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\ &\vdots \\ S_n &= X_1 \cdots X_n \end{aligned}$$

となる．これは**対称式**と呼ばれるものである．これに対し，$K \coloneqq k(S_1, \cdots, S_n) \subseteq L$ とおく．S_i たちは G の作用によってどれも不変なので，K の任意の元も G の作用で不変だから，$K \subseteq L^G$ は分かる．また，$P_n \in K[X]$ である．

$K_i \coloneqq K(X_{n-i+1}, \cdots, K_n)$ とおくと，

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

となる．$P_n(X_n) = 0$ であるから，$[K_1 : K_0] \leq \deg P_n = n$ が成り立つ．ここで，P_n は $K_1[X]$ においては $T - X_n$ でわり切れるから，

$$P_{n-1} \coloneqq \frac{P_n}{T - X_n} \in K_1[X]$$

とおくと，$P_{n-1}(X_{n-1}) = 0$ であるから，$K_2 = K_1(X_{n-1})$ に注意すれば $[K_2 : K_1] \leq \deg P_{n-1} = n - 1$ が分かる．以降これを続けていくことで，

$$[L : K] = [K_n : K_{n-1}] \cdots [K_2 : K_1][K_1 : K_0] \leq 1 \cdot \cdots \cdot (n-1) \cdot n = n!$$

が得られる．一方で $K \subseteq L^G$ より，

$$[L : K] \geq [L : L^G] = \#G = n!$$

であるから，上の式と合わせて $[L : K] = [L : L^G]$ となり，$K = L^G$ が得られる．

10. 2016 年 12 月 13 日

10.1. 1 の冪根と円分多項式

命題 45. 体 K に対し，有限部分群 $M \leq K^\times$ は巡回群であり，その位数は $\operatorname{char} K$ でわり切れない．

$n \coloneqq \#M$ とおく．$n = 1$ なら明らかなので，$n \geq 1$ とする．有限 Abel 群の構造定理により，

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

と書ける．ここで，

$$2 \leq d_1 \mid \cdots \mid d_r; \quad n = d_1 \cdots d_r$$

である．これより，

$$\#\{x \in M \mid x^{d_1} = 1\} = {d_1}^r$$

が分かる．一方で，$X^{d_1} - 1$ は d_1 次式なので，

$$\#\{x \in K^\times \mid x^{d_1} - 1 = 0\} \leq d_1$$

が成り立つ．上の 2 つの式を比べれば ${d_1}^r \leq d_1$ となり，これより $r = 1$ が得られる．すなわち，$M \cong \mathbb{Z}/d_1\mathbb{Z}$ であって巡回群である．

$\operatorname{char} K = 0$ であれば $\#M$ が $\operatorname{char} K$ でわり切れるはずがないので，証明は終わる．$p \coloneqq \operatorname{char} > 0$ とする．M に位数 p の元 x があったとすると，$x^p = 1$ なので，$(x-1)^p = x^p - 1 = 0$ である．したがって，$x - 1 = 0$ より $x = 1$ であるが，1 の位数は p ではないので矛盾である．したがって，M に位数 p の元は存在しないから，$\#M$ は p ではわり切れない．

体 K をとり，$\operatorname{char} K$ でわり切れない正整数 n をとる．L を $X^n - 1$ の K 上分解体とし，

$$M \coloneqq \{x \in L^\times \mid x^n = 1\}$$

とする．$X^n - 1$ とその微分 nX^{n-1} は $n \neq 0$ より互いに素なので，$X^n - 1$ は分離多項式である．したがって $\#M = n$ となり，命題 45 によって $M \cong \mathbb{Z}/n\mathbb{Z}$ となる．

定義 29. 体 K と $\operatorname{char} K$ でわり切れない正整数 n に対し，上記の M の生成元を **1 の原始 n 乗根**といい ζ_n と書く．

この定義によって，

$$M = \{{\zeta_n}^i \mid i = 1, \cdots, n\}$$

と書ける．L は $X^n - 1$ の最小分解体だから，

$$L = K(\zeta_n, {\zeta_n}^2, \cdots, {\zeta_n}^n) = K(\zeta_n)$$

が成り立つ．$X^n - 1$ は分離多項式であったから，L は K の有限次分離拡大である．さらに，多項式の最小分解体なので L は K の正規拡大でもある．したがって，L は K の有限次 Galois 拡大となっている．

さて，$\sigma \in \operatorname{Gal}(L/K)$ をとると，

$$\sigma(\zeta_n)^n - 1 = \sigma({\zeta_n}^n - 1) = 0$$

であるから，M の定義より $\sigma(\zeta_n) \in M$ が成り立つ．すなわち $\sigma(M) \subseteq M$ であるから，写像

$$R\colon\ \operatorname{Gal}(L/K) \to \operatorname{Aut}(M);\ \sigma \mapsto \sigma|_M$$

が定義でき，これは群の準同型写像であって単射である．ここで，M は巡回群だから，

$$F\colon\ \operatorname{Aut}(M) \to (\mathbb{Z}/n\mathbb{Z})^\times;\ i \mapsto \bullet^i$$

は群の同型写像である．なお，$\bullet^i\colon M \to M$ は i 乗写像である．したがって，上の写像の合成 $\Phi \coloneqq F \circ R$ は，群の単射準同型写像 $\Phi\colon \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ になる．これがどのような写像になるかは K に依存する．

以下，$K = \mathbb{Q}$ の場合について，上記で定めた写像 $\Phi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ について調べる．$\mathrm{char}\,\mathbb{Q} = 0$ だから，n は任意の自然数にできる．

定義 30. $\mathbb{Q}$ における原始 n 乗根 ζ_n の $\mathbb{Q}$ 上最小多項式 $P \in \mathbb{Q}[X]$ を n 番目の**円分多項式**という．また，$\mathbb{Q}$ の拡大体 $\mathbb{Q}(\zeta_n)$ を**円分体**という．

命題 46. 任意の n に対し，n 番目の円分多項式は整数係数の多項式である．

ζ_n の最小多項式を $P \in \mathbb{Q}[X]$ とし，$A \coloneqq \mathbb{Z}[\zeta_n] \subseteq \mathbb{Q}(\zeta_n)$ とおく．写像

$$\varphi\colon\ \mathbb{Z}[X] \to A;\ f \mapsto f(\zeta_n)$$

を考えると，${\zeta_n}^n - 1 = 0$ より，写像

$$\tilde{\varphi}\colon\ \mathbb{Z}[X]/\langle X^n - 1\rangle \to A;\ \overline{f} \mapsto f(\zeta_n)$$

が誘導され，これは全射である．$\mathbb{Z}[X]/\langle X^n - 1\rangle$ は $\mathbb{Z}$-加群として $1, X, \cdots, X^{n-1}$ で生成されるから，A も $\mathbb{Z}$-加群としてこれらの像により生成される．したがって，A は有限生成 $\mathbb{Z}$-加群である．また，A は $\mathbb{Q}$-線型空間 $\mathbb{Q}(\zeta_n)$ の部分 $\mathbb{Z}$-加群だから捩れをもたない．$\mathbb{Z}$ は主イデアル整域なので，A は自由 $\mathbb{Z}$-加群である．したがって，A は有限個の $\mathbb{Z}$-基底をもつが，それは $\mathbb{Q}(\zeta_n)$ の $\mathbb{Q}$-基底にもなる．よって，ζ_n 倍写像 $\zeta_n\bullet\colon A \to A$ の固有多項式は，同じく ζ_n 倍写像 $\zeta_n\bullet\colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ の固有多項式でもあり，それは ζ_n の $\mathbb{Q}$ 上最小多項式 P である．ところで，$\zeta_n\bullet\colon A \to A$ の固有多項式は $\mathbb{Z}[X]$ の元だから，$P \in \mathbb{Z}[X]$ が得られた．

定理 47.［Gauss の定理］ 上記の写像 $\Phi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ は同型写像である．

命題 48. n 番目の円分多項式を P_n とすると，

$$X^n - 1 = \prod_{d \mid n} P_d$$

が成り立つ．

定理 47 より，

$$P_n = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} (X - \sigma(\zeta_n)) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - {\zeta_n}^i)$$

が成り立つ．ζ_n が生成する巡回群を M とすれば，$M \cong \mathbb{Z}/n\mathbb{Z}$ だから，

$$S_d \coloneqq \{\zeta \in M \mid \mathrm{ord}\,\zeta = d\}$$

とすると，

$$M = \bigsqcup_{d \mid n} S_d$$

と書ける．したがって，最初の式と合わせて，

$$X^n - 1 = \prod_{\zeta \in M} (X - \zeta) = \prod_{d \mid n} \prod_{\zeta \in S_d} (X - \zeta) = \prod_{d \mid n} \prod_{i \in (\mathbb{Z}/d\mathbb{Z})^\times} (X - {\zeta_n}^i) = \prod_{d \mid n} P_d$$

が得られる．

命題 48 を用いると，円分多項式を簡単に求めることができる．例えば，素数 p に対して $d \mid p$ を満たす d は 1 と p しかないので，

$$X^p - 1 = P_p P_1 = P_p (X - 1)$$

となり，

$$P_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

を得る．番号が小さい方からいくつか具体的に計算すると，

$$\begin{aligned} P_1 &= X - 1 \\ P_2 &= X + 1 \\ P_3 &= X^2 + X + 1 \\ P_4 &= X^2 + 1 \\ P_5 &= X^4 + X^3 + X^2 + X + 1 \\ P_6 &= X^2 - X + 1 \end{aligned}$$

などとなる [*5]．

11. 2016 年 12 月 20 日

11.1. Kummer 拡大

体にある元の冪根を付加した体を考える．一般の議論をする前に，まずは 2 次拡大について調べる．

命題 49. 2 次拡大 L/K をとり，$\operatorname{char} K \neq 2$ とする．このとき，L/K は Galois 拡大で，$\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ である．

L/K は 2 次拡大だから，ある 2 次の既約多項式 $P \in K[X]$ が存在して $L \cong K[X]/\langle P \rangle$ が成り立つ．平方完成により $P =: (X - b)^2 - a$ と表す．$Y := X - b$ とおけば $P = Y^2 - a$ であるから，$P \in K[Y]$ と考えられ，$L \cong K[Y]/\langle P \rangle = K[Y]/\langle Y^2 - a \rangle$ である．P は既約だから，

$$a \notin (K^\times)^2 = \{x^2 \mid x \in K^\times\}$$

[*5] 番号が小さい円分多項式の表示を見ると，係数には 0 か ±1 しか現れないように思えてくるが，それは一般には誤りである．実際，$n \leq 104$ ならば P_n の係数には 0 か ±1 しか現れないが，P_{105} の 41 次および 7 次の係数は −2 である．より強く，任意の整数はある円分多項式の係数に現れることが知られている．

であるから，$L = K(\sqrt{a})$ と書ける．よって，$L[X]$ においては，

$$P = Y^2 - a = (Y - \sqrt{a})(Y + \sqrt{a})$$

と 1 次式の積に分解でき，$\operatorname{char} K \neq 2$ より $\sqrt{a} \neq -\sqrt{a}$ であるから，P は分離多項式であり，L/K は分離拡大である．また，$\sqrt{a}$ の共役は $\pm\sqrt{a}$ であり，これらは L に属するので，L/K は正規拡大である．したがって，L/K は Galois 拡大である．

$\#\mathrm{Gal}(L/K) = 2$ だから，自動的に $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ である．具体的には，

$$\sigma_{\pm}\colon\ K[Y]/\langle Y^2 - a\rangle \to K;\ \overline{f} \mapsto f(\pm\sqrt{a})$$

が $\mathrm{Gal}(L/K)$ の 2 元である．

定義 31. 体 K と $\operatorname{char} K$ でわり切れない正整数 m をとり，$\zeta_m \in K$ であるとする．$a_1, \cdots, a_n \in K^\times$ に対して $L \coloneqq K(\sqrt[m]{a_1}, \cdots, \sqrt[m]{a_n})$ を K の Kummer 拡大という．

命題 50. 体 K と $\operatorname{char} K$ でわり切れない正整数 n をとる．$L \coloneqq K(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_n})$ を K の Kummer 拡大とする．このとき，L/K は Abel 拡大であり，$\mathrm{Gal}(L/K)$ の元は全て n 乗すると 1 になる．

まずは $n = 1$ とし，$L = K(\sqrt[m]{a})$ の場合を考える．$\alpha \coloneqq \sqrt[m]{a}$ とおくと，$L[X]$ において，

$$X^m - a = \prod_{i=1}^{m} (X - {\zeta_m}^i \alpha)$$

と分解できるので，L は $X^m - a$ の最小分解体である．$\alpha \neq 0$ だから，${\zeta_m}^i \alpha$ たちは相異なる．したがって，L/K は分離拡大であり，明らかに正規拡大でもあるので，Galois 拡大になる．ここで，

$$M \coloneqq \{{\zeta_m}^i \mid i = 1, \cdots, m\}$$

とおくと，写像

$$\Phi\colon\ \mathrm{Gal}(L/K) \to M;\ \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

が定義され，群準同型写像になる．$\sigma \in \mathrm{Gal}(L/K)$ が $\Phi(\sigma) = 1$ を満たすとすると，$\sigma(\alpha) = \alpha$ となるが，$L = K(\alpha)$ であって σ は K-準同型写像なので，$\sigma = \mathrm{id}_L$ でなければならない．したがって，Φ は単射である．

一般に $L = K(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_n})$ の場合を考える．$\alpha_j \coloneqq \sqrt[n]{a_j}$ とおく．L は $K(\alpha_j)$ たちの合成体だから，上の議論と命題 37 によって L/K は Galois 拡大である．さらに，上で述べたようにして，単射準同型写像

$$\Phi_j\colon\ \mathrm{Gal}(K(\alpha_j)/K) \to M;\ \sigma \mapsto \frac{\sigma(\alpha_j)}{\alpha_j}$$

を作る．これらは，単射準同型写像

$$\Phi_1 \times \cdots \times \Phi_n\colon\ \mathrm{Gal}(K(\alpha_1)/K) \times \cdots \times \mathrm{Gal}(K(\alpha_n)/K) \to M^{\times n}$$

を構成する．また，

$$\Psi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(K(\alpha_1)/K) \times \cdots \times \mathrm{Gal}(K(\alpha_n)/K);\ \sigma \mapsto (\sigma|_{K(\alpha_1)}, \cdots, \sigma|_{K(\alpha_n)})$$

も明らかに単射準同型写像である．したがって，これらの合成により $\mathrm{Gal}(L/K) \leq M^{\times n}$ と見なせる．$M^{\times n}$ は Abel 群だから，$\mathrm{Gal}(L/K)$ も Abel 群で，L/K は Abel 拡大である．$M^{\times n}$ の元は全て m 乗すると 1 なので，$\mathrm{Gal}(L/K)$ の元もそうである．

12. 2017 年 1 月 10 日

12.1. 方程式の可解性

多項式 $P := X^2 - aX + b \in \mathbb{Q}[X]$ を考えると，その根は

$$\frac{a \pm \sqrt{a^2 - 4b}}{2} \in \mathbb{Q}(\sqrt{a^2 - 4b})$$

であるから，P の根は $\mathbb{Q}$ 上で四則演算と冪根をとる操作によって表示できる．そこで，より一般に $\mathrm{char}\, K = 0$ を満たす体 K に対し，多項式 $P \in K[X]$ の根が，K の元の四則演算と冪根をとる操作によって表示できるかどうか調べたい．ここで，P が可約であれば，既約多項式の積で表してそれぞれの既約多項式について根を調べれば良いので，P が既約である場合を考えれば十分である．

命題 51. 体 K と既約多項式 $P \in K[X]$ をとり，$\mathrm{char}\, K = 0$ とする．また，$L := K[X]/\langle P\rangle$ とおく．このとき，

[1] K の元に四則演算と冪根をとる操作を有限回施すことで，P の全ての根を表示できる

[2] K の有限次拡大の列

$$K = K_0 \leq K_1 \leq \cdots \leq K_m$$

が存在し，K_i に 1 の原始 n_i 乗根が属していて，ある $a_i \in K_i$ によって $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ が成り立ち，$L \subseteq K_m$ が成り立つ

[3] K の有限次 Galois 拡大の列

$$K = K'_0 \leq K'_1 \leq \cdots \leq K'_{m'}$$

が存在し，$\mathrm{Gal}(K'_{i+1}/K'_i)$ は Abel 群であり，$L \subseteq K'_{m'}$ が成り立つ

[4] Galois 群が可解群となるような K の Galois 拡大に L が含まれる

は同値である．

[1]⇔[2]: P の根を a とすれば $L = K(a)$ だから，この同値性は明らかである．

[2]⇒[3]: K_{i+1}/K_i が Kummer 拡大となっているから，命題 50 より K_{i+1}/K_i は Abel 拡大であり，すなわち $\mathrm{Gal}(K_{i+1}/K_i)$ は Abel 群である．また，K_{i+1}/K_i は特に Galois 拡大であるから，順に K_i/K も Galois 拡大である．したがって，条件 3 が示された．

[3]⇒[2]:

[3]⇒[4]: $G \coloneqq \mathrm{Gal}(K'_{m'}/K)$ および $G_i \coloneqq \mathrm{Gal}(K'_{m'}/K'_i)$ とおくと，群の列

$$G = G_0 \geq G_1 \geq \cdots \geq G_{m'} = 1$$

ができる．K'_{i+1}/K'_i は Galois 拡大だから，命題 43 によって $G_i \trianglerighteq G_{i+1}$ である．また，

$$G_i/G_{i+1} = \mathrm{Gal}(K'_{m'}/K'_i)/\mathrm{Gal}(K'_{m'}/K'_{i+1}) \cong \mathrm{Gal}(K'_{i+1}/K'_i)$$

であり，これは主張から Abel 群である．したがって，列 $(G_i)_{0\leq i\leq m'}$ は G の Abel 正規列になっており，これより G は可解群である．これより，条件 4 が示された．

[4]⇒[3]:

定義 32. 体 K が $\mathrm{char}\, K = 0$ を満たすとする．n 変数有理関数体 $L \coloneqq K(a_0, \cdots, a_{n-1})$ に係数をもつ多項式

$$P \coloneqq X^n - a_{n-1}X^{n-1} + \cdots + (-1)^n a_0 \in K(a_0, \cdots, a_{n-1})[X]$$

を K 上 n 次**一般多項式**という．

上記の定義において，K 上一般多項式 P の根が，L の元に四則演算と冪根をとる操作を施すことで表せるとは，すなわち K 係数多項式の根の公式が存在するということである．2 次多項式であれば，よく知られた根の公式

$$X = \frac{-a_1 \pm \sqrt{{a_1}^2 - 4a_0}}{2}$$

が存在する．

命題 52. K 上 n 次一般多項式 P をとり，その係数を付加した体を L とする．このとき，$L[X]/\langle P\rangle$ は L の有限次 Galois 拡大であり，その Galois 群は n 次対称群 S_n と同型である．

定理 53. n 次一般多項式の全ての根が，係数に対し四則演算と冪根をとる操作を有限回施すことによって表示できるための必要十分条件は $n \leq 4$ である．

S_n が可解となるための必要十分条件が $n \leq 4$ であるから，命題 52 から明らかである．

定理 53 により，5 次以上の多項式には根の公式が存在しないことが示された．一方，4 次以下の多項式については根の公式が存在することになるが，その具体的な式については Cardano と Ferrari などによって与えられている．

12.2. 代数閉包

定義 33. 体 K 上の既約多項式が 1 次式のみであるとき，K を**代数閉体**という．

命題 54. 体 K について，

[1] K は代数閉体である

[2] K の有限次拡大は K 自身のみである

[3] 定数でない K 上多項式は K に根をもつ

は同値である．

定義 34. 体 K に対し，K の代数拡大で代数閉体であるものを K の**代数閉包**といい，それを $\overline{K}$ で表す．

命題 55. 体 K と K の代数拡大 L に対し，

[1] L は代数閉体である

[2] $K[X]$ の 0 でない任意の元は $L[X]$ において 1 次式の積に分解する

[3] $K[X]$ の定数でない任意の元は L において根をもつ

は同値である．

定理 56.［Steinitz の定理］ 任意の体 K に対し，K の代数閉包は同型を除いて一意に存在する．

以下，

$$K[X]^* := \{f \in K[X] \mid f \text{ は定数でないモニック多項式 }\}$$

とする．各 $f \in K[X]^*$ に対して不定元 X_f を作り，これら全てから作られる多項式環

$$A := K[X_f \mid f \in K[X]^*]$$

を考える．A において $f(X_f) \in A$ $(f \in K[X]^*)$ たちが生成するイデアルを

$$\mathfrak{a} := \langle f(X_f) \mid f \in K[X]^* \rangle \leq A$$

とおき，$B := A/\mathfrak{a}$ とする．

もし $\mathfrak{a} = A$ であれば $1 \in \mathfrak{a}$ であるから，$f_i \in K[X]^*$ たちと $g_i \in A$ たちによって，

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

が成り立つ．$f_1 \cdots f_n \in K[X]$ の K 上最小分解体を L とおくと，各 f_i は根 $a_i \in L$ をもつ．そこで，上の式において，各 X_{f_i} には a_i を代入し，g_i たちの中に現れるそれ以外の不定元には 0 を代入すれば，L において $0 = 1$ となり矛盾する．したがって，$\mathfrak{a} \neq A$ であるから $B \neq 0$ である．

これにより，選択公理を用いて B の極大イデアル $\mathfrak{m}$ をとると，$M := B/\mathfrak{m}$ は体である [*6]．作り方か

[*6] 極大イデアルをとるのに選択公理が必要となる．ただし，K の濃度が高々可算であれば，その代数閉包の存在は選択公理を使わずに証明できることが知られている．

ら $M = K(\overline{X_f} \mid f \in K[X]^*)$ であり，任意の $f \in K[X]^*$ に対して M において $f(\overline{X_f}) = 0$ が成り立つ．したがって，M は K の代数拡大であって，命題 55 の条件 3 と条件 1 の同値性により M は代数閉体だから，M は K の代数閉包になる．

定理 57. $\mathbb{R}$ の代数閉包は $\mathbb{C}$ である．

12.3. 超越次数

定義 35. 拡大 L/K と元 $x_1, \cdots, x_n \in L$ に対し，写像

$$\varphi\colon\ K[X_1, \cdots, X_n] \to L;\ f \mapsto f(x_1, \cdots, x_n)$$

が単射であるとき，$x_1, \cdots, x_n$ は K 上**代数的独立**であるという．

定義 36. 拡大 L/K と元 $x_1, \cdots, x_n \in L$ をとる．$x_1, \cdots, x_n$ が K 上代数的独立で，L が $K(x_1, \cdots, x_n)$ 上代数的であるとき，$x_1, \cdots, x_n$ を L の K 上という．

命題 58. 拡大 L/K に対し，L が K 上体として有限生成であれば，L の K 上超越基底は存在する．

命題 59. 拡大 L/K に対し，L の K 上超越基底は存在すればその個数は一定である．

定義 37. 拡大 L/K に対し，L の K 上超越基底の個数を L の K 上**超越次数**といい，それを $\mathrm{trdeg}_K L$ で表す．超越基底が存在しない場合は，$\mathrm{trdeg}_K L = \infty$ とする．

なお，超越基底の定義は個数が一般の濃度になる場合にも拡張でき，その場合は任意の拡大 L/K に対して L の K 上超越基底が存在する．

索引