12 Galois 拡大再論

12.1 Galois 拡大

命題 12.1. 代数拡大 L/K について次は同値

(1) L/K は Galois

(2) L/K は正規かつ分離的

(2)′ $^\forall x \in L$ に対し、その最小多項式は分離的かつ $L[X]$ において一次因子の積に分解される。

(3) L/K はある分離多項式族 $(f_i)_{i\in I}$ の最小分解体

さらに、 L/K が有限次なら次も同値

(4) $[L:K] = h_L(L)(:= |\operatorname{Aut}_K(L)|)$

Proof. Ω を K の代数閉包とする。

(2) $\Leftrightarrow$ (2)′ は正規の定義 (**??**) と系 (**??**) と多項式の分離性の定義 (**??**) から明らか。

(1) $\Rightarrow$ (2)

$^\forall x \in L$ とその最小多項式 $f \in K[X]$ をとる。また、$Y_x := \{\sigma(x) | \sigma \in \operatorname{Aut}_K(L)\}$ と定めるとこれは x の Ω における共役元の集合の部分集合になり、$\sigma \in \operatorname{Aut}_K(L)$ から $Y \subset L$ である。命題 (**??**) の (1) $\Leftrightarrow$ (3) から x の共役元はすべて f の根なので高々 $\deg(f)$ 個しかないので Y_x は有限集合。$g := \prod_{y\in Y_x}(X-y), n := \deg(g)$ とする。y はすべて異なるから単根なので g は分離的である。また、 y は x の共役元より f の根でもあるから g のすべての根は f の根より $g|f$ となる。

$y \in Y_x \subset L$ よりその元から作られる基本対称式は L に含まれるので $g = \sum_{i=1}^n a_i X^i, a_i \in L$ と書ける。$\sigma g = \sum_{i=1}^n \sigma(a_i)X^i$ とすると係数だけに σ をかけているから $(\sigma g)(X) = \prod_{y\in Y_x}(X - \sigma(y))$ となる。ここで $y \in Y_x$ より $y = \tau(x), \tau \in \operatorname{Aut}_K(L)$ となるものが存在する。$\operatorname{Aut}_K(L)$ は自己同型写像であるから $\sigma\circ\tau \in \operatorname{Aut}_K(L)$ より $\sigma(y) = \sigma\circ\tau(x) \in Y_x$ となる。ここで Y_x は有限集合であることと σ は体の準同型より単射なのでそれぞれの y は σ によりそれぞれ異なる Y_x の元に行く。したがって $(\sigma g)(X) = \prod_{y\in Y_x}(X-y) = g(X)$ となるから a_i は $^\forall\sigma \in \operatorname{Aut}_K(L)$ によって動かされない。L/K が Galois より $L^{\operatorname{Aut}_K(L)} = K$ より $a_i \in K$ であるから $g \in K[X]$ である。

$g, f \in K[X]$ で $g|f$ より f の最小性から $f = g$ なので任意の $x \in L$ の最小多項式は $f = \prod_{y\in Y_x}(X-y)$ と $L[X]$ 上で一次因子の積に分解されるので L/K は正規。また、 $g(=f)$ は分離的でもあったので任意の最小多項式が分離的より系 (**??**) より L/K は分離的であるので L/K は正規かつ分離的。

(2) $\Rightarrow$ (1)

$L = K$ のとき $L^{\operatorname{Aut}_K(L)} = K^{\operatorname{Aut}_K(K)} = K$ で成立。$L \neq K$ のとき $L \supsetneq K$ であるから $^\forall x \in L - K$ をとる。これがある $\sigma \in \operatorname{Aut}_K(L)$ で $\sigma(x) \neq x$ となればよい。

x の最小多項式を $f \in K[X]$ とすると $x \in L - K$ より $\deg(f) > 1$ であり、仮定から L/K が分離的より系 (**??**) から f が単根を持つので定義より分離的だから $f(y) = 0$ で $y \neq x$ であるような元 $y \in \Omega$ が存在する。y の K 上の最小多項式も f なので命題 (**??**) の (2) $\Leftrightarrow$ (3) から $\sigma(x) = y$ となるような $\sigma \in \operatorname{Aut}_K(\Omega)$ が存在する。仮定から L/K は正規なので命題 (**??**) の (1) $\Leftrightarrow$ (3) から $\sigma(L) = L$ より $\sigma|_L \in \operatorname{Aut}_K(L)$ となる。この σ により $\sigma(x) = y \neq x$ なので x は固定されないから固定されるのは K の元のみなので $L^{\operatorname{Aut}_K(L)} = K$ となり定義より L/K は Galois である。

(2) $\Leftrightarrow$ (3)

命題 (**??**) の (1) ⇔ (5) より「規 ⇔ ある多項式族 $(f_i)_{i\in I}$ の最小分解体」が言えている。その多項式族は $^\forall x \in L$ の最小多項式の族であったので系 (**??**) より「分離的 ⇔ 多項式族のすべての多項式が分離的」が言えている。

(2) ⇔ (4)

有限次拡大のとき系 (**??**) から「正規 ⇔ $[L:K]_s = h_L(L)$」が言えている。定義より「分離的 ⇔ $[L:K] = [L:K]_s$」なので「正規かつ分離的 ⇔ $[L:K] = [L:K]_s = h_L(L)$」となり示された。 □

12.2 多項式の Galois 群

定義 12.2. K : 体、 $f \in K[X] - K$: 分離多項式、 L_f : f の K 上の最小分解体とするときその根をすべて添加しているので命題 (**??**) から L_f/K は有限次だから命題 (12.1) の (1) ⇔ (3) から L_f/K は有限次 Galois 拡大である。このとき $\mathrm{Gal}(L_f/K)$ をf の K 上の Galois 群という。

命題 12.3. 分離多項式 $f \in K[X] - K$ にたいしてその最小分解体 L_f を考える。Ω を K の代数閉包で L_f を含むもの、$W := \{x \in \Omega | f \text{ の根 }\}$ とする。f は分離多項式なので $|W| = n := \deg(f)$ となる。このとき $\mathrm{Gal}(L_f/K)$ は W に作用し、根の置換を引き起こす。したがって W の自己同型写像の群、つまり W の置換群を $\mathfrak{S}_W$ とするとき $|W| = n$ から n 次対称群 $\mathfrak{S}_n$ でもあり、

$$\begin{aligned} \mathrm{Gal}(L_f/K) &\longrightarrow \mathfrak{S}_W (= \mathfrak{S}_n) \\ \sigma &\longmapsto \sigma|_W \end{aligned}$$

という単射群準同型が存在する。 ($\mathfrak{S}_W$に $\mathrm{Gal}(L_f/K)$ は埋め込める)

とくに $|\mathrm{Gal}(L_f/K)| = [L_f : K] \leq n!$ である。

Proof. $^\forall \sigma \in \mathrm{Gal}(L_f/K) = \mathrm{Aut}_K(L_f)$ は $f(\sigma(x)) = \sigma(f(x)) = 0$ より $\sigma(x) \in W$ だから $\sigma(W) \subset W$ なので

$$\begin{aligned} \sigma|_W : W &\longrightarrow W \\ x &\longmapsto \sigma(x) \end{aligned}$$

となり σ は体の準同型より単射であって $|W| = n$ で有限集合なのでこれは全単射である。したがって $\sigma|_W$ は W 上の全単射写像の群である $\mathfrak{S}_W$ の元となる。$\sigma = \tau \in \mathrm{Gal}(L_f/K)$ のとき、 $\sigma|_W = \tau|_W$ であるので $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W, \sigma \longmapsto \sigma|_W$ は写像になっている。また、 $\sigma|_W = \tau|_W$ のとき、$\mathrm{Aut}_K(L_f)$ の元としての σ, τ は K を動かさないので最小分解体の定義から $L_f = K(W)$ なので W の動かし方で定まるから $\sigma = \tau$ である。したがって制限写像 $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W$ は単射である。

L_f/K は定義 (12.2) から有限次 Galois なので命題 (12.1) の (1) ⇔ (4) から $[L_f : K] = h_{L_f}(L_f) = |\mathrm{Aut}_K(L_f)| = |\mathrm{Gal}(L_f/K)|$ である。ここで上述のことから $\mathrm{Gal}(L_f/K)$ は $\mathfrak{S}_W = \mathfrak{S}_n$ に埋め込めるから $|\mathrm{Gal}(L_f/K)| = [L_f : K] \leq |\mathfrak{S}_n| = n!$ より示された。 □

系 12.4. 一般の n 次多項式 $f \in K[X]$ の最小分解体 L の拡大次数は $n!$ 以下である。

Proof. 命題 (12.3) で f は分離多項式とは限らないので $|W| \leq n$ であるから $|\mathfrak{S}_W| \leq |\mathfrak{S}_n|$ である。埋め込むことは同様にできるから $\mathrm{Gal}(L_f/K)$ を $\mathrm{Aut}_K(L)$ として $|\mathrm{Aut}_K(L)| \leq |\mathfrak{S}_W| \leq |\mathfrak{S}_n| = n!$ より成立。 □

命題 12.5. 分離多項式 $f \in K[X] - K$ の根の集合 W とその元 $x, y \in W$ に対して以下は同値。

(1) x と y は K 上共役。

(2) x と y は同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属する。

(3) x と y は f の同じ既約成分の根。

とくに f が既約であるためには $W \neq \emptyset$ かつ $\mathrm{Gal}(L_f/K)$ が W に推移的に作用することが必要十分である。(群 G が集合 X に推移的に作用するとは $G-$ 軌道 $G(x) := \{\sigma(x)|\sigma \in G\}$ とするとき $G(x) = X$ となること)

Proof. Ω を K の代数閉包とする。

(1) $\Leftrightarrow$ (2)

f が分離的なので L_f/K は有限次 Galois 拡大であるから正規なので $\sigma \in \mathrm{Aut}_K(\Omega), \sigma(L_f) = L_f$ を満たすから $\sigma|_{L_f} \in \mathrm{Aut}_K(L_f) = \mathrm{Gal}(L_f/K)$ となる。また、 $\sigma \in \mathrm{Gal}(L_f/K)$ は系 (**??**) より $\tilde{\sigma} \in \mathrm{Aut}_K(\Omega)$ に拡張できる。これより

$$\begin{aligned} x \text{ と } y \text{ が } K \text{ 上共役} &\Leftrightarrow {}^{\exists}\sigma \in \mathrm{Aut}_K(\Omega), x = \sigma(y) \\ &\Leftrightarrow y \in \{\sigma(x)|\sigma \in \mathrm{Gal}(L_f/K)\} \\ &\Leftrightarrow y \text{ は } x \text{ の } \mathrm{Gal}(L_f/K) - \text{軌道に含まれる} \end{aligned}$$

となる。

(1) $\Leftrightarrow$ (3)

命題 (**??**) の (1) $\Leftrightarrow$ (3) より x と y が K 上共役 $\Leftrightarrow$ x と y の K 上の最小多項式は同じなのでその最小多項式を $g \in K[X] - K$ とすれば g は f の既約成分であるので示された。

もし $\mathrm{Gal}(L_f/K)$ が $W(\neq \emptyset)$ に推移的に作用するとすると、ある f の根 x に対してその $\mathrm{Gal}(L_f/K)-$ 軌道は W に一致するので任意の f の根は (2) $\Leftrightarrow$ (3) から f の同じ既約成分の根になる。したがって f の根はすべて f の既約成分の根になるから f は既約。f が既約であるとき (2) $\Leftrightarrow$ (3) からすべての根はある f の根 x と同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属するから $W \subset \mathrm{Gal}(L_f/K)-$ 軌道である。また、 x の軌道はすべて f の根になるから $W \supset \mathrm{Gal}(L_f/K)-$ 軌道より $W = \mathrm{Gal}(L_f/K)-$ 軌道となり推移的である。 □

例 12.6. K : 体、 $L := K(T_1, \ldots, T_n)$: n 変数の有理関数体とする。$G := \mathfrak{S}_n$ として T_i の添字の置換とする。つまり、 $\sigma \in G$ と $f = f(T_1, \ldots, T_n) \in L$ に対して、$\sigma f := f(T_{\sigma(1)}, \ldots, T_{\sigma(n)})$ と作用させることとする。このとき、 G の元は T_i を写し、 K の元は動かさないので L の体の自己同型とみなせるので $G \subset \mathrm{Aut}_{\text{体}}(L)$ となる。

$M := L^G$ とおくとこれは $T_1, \ldots, T_n$ の対称有理式の集合になる。このとき L/M が Galois となって、$G = \mathrm{Gal}(L/M)$ を満たす。とくに $[L : M] = n!$ となる。

Proof. $s_i := (T_1, \ldots, T_n$の i 次基本対称式) とすると $s_i \in L$ である。つまり、 $s_1 = T_1 + \cdots + T_n, s_2 = T_1T_2 + T_1T_3 + \cdots + T_{n-1}T_n, \cdots, s_n = T_1 \cdots T_n$ となっている。$M_0 := K(s_1, \ldots, s_n)$ とおくと基本対称式は文字を置換しても同じままなので M_0 は G で固定される。よって $M_0 \subset M$ である。

ここで $T_1, \ldots, T_n$ は解と係数の関係から $X^n - s_1X^{n-1} + \cdots + (-1)^n s_n \in M_0[X]$ の根になる。$T_1, \ldots, T_n$ はそれぞれ異なるから命題 (**??**) からこの多項式は分離的である。L はこの多項式の最小分解体なので定義 (12.2) から L/M_0 は有限次 Galois 拡大になる。命題 (12.3) から $[L : M_0] \leq n!$ である。また、 L/M は Artin の定理 (**??**) から Galois 拡大で $G = \mathfrak{S}_n = \mathrm{Aut}_M(L)$ であり、Rem (**??**) から $[L : M] = |\mathrm{Aut}_M(L)| = |\mathfrak{S}_n| = n!$ となる。よって $M_0 \subset M$ と $[L : M_0] \leq n! = [L : M]$ より $M_0 = M$ となる。以上より M は $T_1, \ldots, T_n$ の対称有理式の集合になり、$G = \mathfrak{S}_n = \mathrm{Gal}(L/M)$ で、 $[L : M] = n!$ となる。 □

Fact 12.7. $n \geq 5$ ならば n 次交代群 $\mathfrak{A}_n$ は非アーベル単純群なので非自明な正規部分群を持たない。命題 (**??**) より可解群となるための可解列に出てくる交換子群は正規部分群であるので $\mathfrak{A}_n$ は可解群にならない。よって $\mathfrak{A}_n$ を含む $\mathfrak{S}_n$ は $n \geq 5$ で非可解群。任意の n 次分離多項式 ($\in \mathbb{Q}[X]$) の Galois 群は命題 (12.3) より $\mathfrak{S}_n$ の部分群に同型である。これより定理 **??** から 5 次以上の一般代数方程式は解の公式を持たないことがわかる。

12.3 IGP (Inverse Galois Problem)

Galois の逆問題 (IGP Inverse Galois Problem) とは K : 体、G : 有限群が与えられたとき、$\mathrm{Gal}(L/K) \cong G$ となる Galois 拡大 L/K は作れるかというもの

Fact 12.8. Hilbert の既約性定理
$X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$ はほとんどの (有限個の例外を除き) $(s_1, \ldots, s_n) \in \mathbb{Q}^n$ に対し既約でその Galois 群は $\mathfrak{S}_n$ と同型。

12.4 無限次 Galois 拡大

L/K が無限次 (かもしれない)Galois 拡大のとき $\mathrm{Gal}(L/K)$ は profinite(副有限、射影有限) 群 (有限群の射影極限になっている群) である。つまり、 $L'/K, L''/K(L' \subset L'')$ を L に含まれる任意の有限次 Galois 拡大とし、制限写像 $\mathrm{Gal}(L''/K) \longrightarrow \mathrm{Gal}(L'/K), \sigma \longmapsto \sigma|_{L'}$ による射影極限

$$\mathrm{Gal}(L/K) = \varprojlim_{L'/K} \mathrm{Gal}(L'/K) \subset \prod_{L'/K} \mathrm{Gal}(L'/K)$$

で定義される。$\mathrm{Gal}(L'/K)$ は離散位相によって位相群になるので $\mathrm{Gal}(L/K)$ にはその直積位相が入り、これを Krull 位相という。

定理 12.9. Galois 理論の基本定理の無限次版
L/K :Galois 拡大、 $G := \mathrm{Gal}(L/K)$ とすると次の一対一対応がある。

$$\begin{aligned}
\{L/K \text{ の部分体 }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の閉部分群 }\} \\
M &\longmapsto \mathrm{Aut}_M(L) = \mathrm{Gal}(L/M) \\
L^H &\longmapsfrom H \\
\{L/K \text{ の部分体で } K \text{ 上有限次のもの }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の開部分群 (指数有限の部分群)}\} \\
\{L/K \text{ の部分体で } K \text{ 上有限次のものでかつ } K \text{ 上 Galois になるもの }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の開正規部分群 }\}
\end{aligned}$$

他の性質は有限次のとき (**??**) と同じ。

定義 12.10. K : 体、K^{sep} : K の分離閉包とするとき、命題 (**??**) から K の代数閉包の相対的分離閉包が K^{sep} になるから $^\forall x \in K^{\mathrm{sep}}$ は K 上代数的かつ分離的なので K^{sep}/K は Galois であり、$G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ を K の絶対 Galois 群という。

すると、 L'/K を K^{sep}/K に含まれる有限次 Galois 拡大とするとき $G_K = \varprojlim_{L'/K} \mathrm{Gal}(L'/K)$ となり、とく

に ${}^\forall L'/K$ に対し $G_K \xrightarrow{sur} \mathrm{Gal}(L'/K)$ があるから ${}^\forall L'/K$ に G_K が作用していると考えられる。
逆に G_K から K を作ることも考えられる。

定理 12.11. Neukirch − 内田 (−Pop) の定理
K_1, K_2 : 素体上有限生成な体。

$$G_{K_1} \cong G_{K_2} \Rightarrow K_1 \cong K_2$$
(位相群として同型)　(体として同型)

が成り立つ。これの一般化である Grothendieck 予想もある。

12.5 有限体の Galois 拡大

以下では K : 有限体、 $\mathrm{char}(K) = p > 0$ で $[K : F_p] = f, |K| = p^f = q$ とする。

定義 12.12. 群 G の冪数とはそれが存在するなら G の元の位数の最小公倍数のことである。

補題 12.13. 体 F の乗法群 $F^\times$ の有限部分群は巡回群。

Proof. G を $F^\times$ の有限部分群、 N を G の冪数とする。このとき正整数 $n_1|n_2|\cdots|n_r$ によって $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \mathbb{Z}/n_r\mathbb{Z}$ で $N = \mathrm{LCM}(n_1, \ldots, n_r) = n_r$ となる。このとき ${}^\forall x \in G, x^N = 1$ より G の元は $X^N - 1$ の根であり、この多項式は F に高々 N 個しか根を持たないので $|G| \leq N$ となる。そして、$|\mathbb{Z}/n_r\mathbb{Z}| = n_r = N$ より $G = \mathbb{Z}/n_r\mathbb{Z}$ となるしかなく、したがって G は巡回群になる。 □

系 12.14. K が q 元体ならば $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$ で位数 $q-1$ の巡回群となる。

Proof. $K^\times$ は 0 を除いた $q-1$ 個の元の有限群なので成立。 □

系 12.15. 位数 q の有限体 K は同型を除き一意に定まる。これを $\mathbb{F}_q$ と書く。

Proof. 有限体 K は素体として $\mathbb{F}_p$ と同型な体を含む。Ω を $\mathbb{F}_p$ の代数閉包とすると $K/\mathbb{F}_p$ が有限次拡大より代数拡大なので定理 (**??**) から Ω に K を埋め込める。K の元は系 (12.14) より $X^{q-1} - 1$ の根と 0 ですべて出しつくされるので $K = \{x \in \Omega | x^q = x\}$ と書ける。Ω に埋め込めばすべてこの形に書けるので同型を除き一意に定まる。 □

系 12.16. 各 $n \in \mathbb{Z}^+$ に対し $\mathbb{F}_q$ の n 次拡大は同型を除きただ一つ存在しそれは $\mathbb{F}_{q^n}$ である。とくに $\mathbb{F}_p$ の代数閉包 Ω の中では唯一つである。

Proof. $\mathbb{F}_q$ の n 次拡大は $\mathbb{F}_p$ の q^n 次拡大なので系 (12.15) を q^n について適用すれば良い。Ω の中では $\mathbb{F}_{q^n} = \{x \in \Omega | x^{q^n} = x\}$ として書けるので唯一つに定まる。 □

命題 12.17. $\mathbb{F}_{q^n}/\mathbb{F}_q$ は Galois 拡大であり

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$
$$1 \longmapsto \phi_q$$

で定める準同型写像は同型写像になる。ただし、 ϕ_q は

$$\begin{aligned}\phi_q : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n}\\ x &\longmapsto x^q\end{aligned}$$

とする。

Proof. $\mathbb{F}_q$ の任意の n 次拡大体 L は系 (12.16) より $L \cong \mathbb{F}_{q^n}$ となるので $L = \mathbb{F}_{q^n}$ とする。定義から $\phi_q \in \mathrm{Aut}(\mathbb{F}_{q^n})$ である。$^\forall x \in \mathbb{F}_q$ に対しては $\mathbb{F}_q = \{x \in \Omega | x^q = x\}$ より $\phi_q(x) = x^q = x$ なので $\mathbb{F}_q$ 上恒等的だから $\phi_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ となる。

また、 ϕ_q は位数 n になることを示す。つまり、 ϕ_q^i が $i = 1, \ldots, n-1$ で $\phi_q^i \neq \mathrm{Id}$ となり、$i = n$ で $\phi_q^i = \mathrm{Id}$ となればよい。$\phi_q^i : x \longmapsto \phi_q^i(x) = x^{q^i}$ であるからもしこれが恒等であるとすると $^\forall x \in \mathbb{F}_{q^n}, x^{q^i} = x$ であるので $\mathbb{F}_{q^n}$ は系 (12.16) の証明における $\{x \in \Omega | x^{q^i} = x\} = \mathbb{F}_{q^i}$ の部分集合になるから元の個数を考えれば $i = n$ でそのようになることがわかる。したがって ϕ_q は位数 n である。

$G := \langle \phi_q \rangle \subset \mathrm{Aut}(\mathbb{F}_{q^n})$ とする。ϕ_q の位数が n より $\langle \phi_q \rangle \cong \mathbb{Z}/n\mathbb{Z}$ となる。L/L^G は Artin の定理 (**??**) より Galois 拡大で $[L : L^G] = |G| = n$ となる。また、 $L = \mathbb{F}_{q^n}$ より $[L : \mathbb{F}_q] = n$ なので $[L : \mathbb{F}_q] = [L : L^G]$ と $\mathbb{F}_q, L^G \subset L$ より $\mathbb{F}_q = L^G$ となるから $\mathbb{F}_{q^n}/\mathbb{F}_q$ は Galois 拡大でその Galois 群は $\mathbb{Z}/n\mathbb{Z}$ と同型。 □

系 12.18. $\mathbb{F}_q$ の代数閉包を $\overline{\mathbb{F}_q}$ とすると $\mathbb{F}_q$ の絶対 Galois 群 $G_{\mathbb{F}_q} := \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ であり、このとき $G_{\mathbb{F}_q} \cong \hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ となる。また、 $\mathbb{Z}_l := \varprojlim_m \mathbb{Z}/l^m\mathbb{Z}$ とするとき $\hat{\mathbb{Z}}$ は $\prod_{l:\text{素数}} \mathbb{Z}_l$ とも書ける。

例 12.19. 形式的冪級数体 $K := \mathbb{C}((X))$ の絶対 Galois 群は $G_K \cong \hat{\mathbb{Z}}$ である。

12.6 円分拡大

定義 12.20. K : 体、 $n \in \mathbb{Z}^+$ とする。

$X^n - 1 \in K[X]$ の K 上の最小分解体を K のn 分拡大 (n − th cyclotomic extension)といい、ある n に対する n 分拡大を円分拡大 (cyclotomic extension)という。とくに $K = \mathbb{Q}$ のとき n 分体、円分体という。

$p \mid n$ のとき、 $n = p^e m$ かつ $p \nmid m$ となる $e, m \in \mathbb{Z}^+$ が存在して、 $X^n - 1 = X^{p^e m} - 1 = (X^m - 1)^{p^e}$ となるので $X^n - 1$ の最小分解体と $X^m - 1$ の最小分解体は一致するから以降は $p \nmid n$ で考える。

$X^n - 1 \in K[X]$ が分離的であるときは定義 (12.2) より有限次 Galois 拡大である。

補題 12.21. $\mathrm{char}(K) = p > 0$ であるとき $X^n - 1 \in K[X]$ について以下は同値。

(1) $p \nmid n$

(2) $X^n - 1$ は分離的。

Proof. 命題 (**??**) の (1) ⇔ (4) より $X^n - 1$ は分離的 ⇔ $X^n - 1 \notin K[X^p]$ ⇔ $p \nmid n$ なので成立。 □

Rem 12.22. 補題 (12.21) の同値からいま $p \nmid m$ で考えてるので $X^n - 1$ は分離的だから円分拡大は Galois 拡大になる。

定義 12.23. K の元 ζ が 1 の n 乗根とはある $n \in \mathbb{Z}^+$ に対して $\zeta^n = 1$ となることである。原始 n 乗根とは ζ の位数が n であることである。つまり原始 n 乗根は n 乗して初めて 1 になる K の元のこと。

補題 12.24. K の代数閉包を Ω とし、それに含まれる $1 (\in K)$ の n 乗根全体の集合を $\mu_n (:= \{1$ の n 乗

根 $\in \Omega\}$) とする。このとき μ_n は K の積で群を成す。これは原始 n 乗根をもち、それの冪乗で任意の μ_n の元を表せる。

Proof. 結合法則は K より成り立つ。$\zeta_i, \zeta_j \in \mu_n$ に対して $(\zeta_i\zeta_j)^n = \zeta_i^n\zeta_j^n = 1 \cdot 1 = 1$ より $\zeta_i, \zeta_j \in \mu_n$ なので積で閉じている。単位元は $1 \in K$ が $1^n = 1$ より存在している。$\zeta_i\zeta_i^{n-1} = \zeta_i^n = 1$ から $\zeta_i^{-1} = \zeta_i^{n-1}$ から逆元が存在するので μ_n は群。

とくにこれは $K^\times$ の有限部分群なので補題 (12.13) から巡回群になるので生成元 $\zeta \in \mu_n$ が存在する。これは位数 n なので定義 (12.23) から原始 n 乗根である。したがって $|\mu_n| \leq n$ と ζ の位数が n より $|\mu_n| = n$ で $^\forall x \in \mu_n$ に対して $x = \zeta^i$ となる $j \in \mathbb{Z}, 1 \leq i \leq n$ が存在する。 □

補題 12.25. 補題 (12.24) の文字を用いて $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ が成り立つ。

Proof. ζ は μ_n の生成元なので $\zeta_i := \zeta^i$ とする。このとき

$$\begin{aligned} \phi : \mu_n &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \zeta_i = \zeta^i &\longmapsto i \end{aligned}$$

とすると $\zeta^i = \zeta^j$ のとき $\zeta^i\zeta^{n-i} = \zeta^j\zeta^{n-i} \Leftrightarrow 1 = \zeta^{n+j-i} \Leftrightarrow 1 = \zeta^{j-i}$ より $j - i \in n\mathbb{Z}$ から $j = i \in \mathbb{Z}/n\mathbb{Z}$ なので写像になっている。$i = j$ のとき $\zeta^i = \zeta^j$ より単射で $^\forall i \in \mathbb{Z}/n\mathbb{Z}$ で $1 \leq i \leq n$ だから $\zeta^i \in \mu_n$ を取ればいいから全射。また、 $\phi(\zeta^i\zeta^j) = \phi(\zeta^{i+j}) = i + j, \phi(\zeta^i) + \phi(\zeta^j) = i + j$ より群準同型になっているため $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ である。 □

補題 12.26. 補題 (12.24) の文字を用いて $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ が成り立つ。

Proof. μ_n 上で

$$\begin{aligned} \phi : \mu_n &\longrightarrow \mu_n \\ \zeta(:= \zeta_1) &\longmapsto \phi(\zeta) \\ \zeta_i &\longmapsto \phi(\zeta_i) = \phi(\zeta)^i (1 \leq i \leq n) \end{aligned}$$

とすると μ_n の元は ζ の冪で全て表せるので ϕ が一意に定まり、準同型になる。もし $\phi(\zeta)$ が μ_n の原始 n 乗根でないとするとある $1 \leq j \leq n$ で $\phi(\zeta)^j = 1$ となる。しかし、 ϕ が準同型より $\phi(\zeta^j) = 1$ から $\zeta^j = 1$ となりこれは ζ が原始 n 乗根であることに矛盾するので $\phi(\zeta)$ も原始 n 乗根である。$\phi(\zeta) \in \mu_n$ より $\phi(\zeta) = \zeta^a$ となる $a \in \mathbb{Z}^+, 1 \leq a \leq n$ が存在している。$a = 1$ となると a と n は互いに素であるから $a \in (\mathbb{Z}/n\mathbb{Z})^*$ である。$a \neq 1$ のとき $a \mid m$ であるとすると $ak = n$ となる $k \in \mathbb{Z}^+, 1 \leq k < n$ があり $a = n/k$ となる。$\phi(\zeta)^k = (\zeta^{n/k})^k = \zeta^n = 1$ となり、これは $\phi(\zeta)$ が原始 n 乗根であることに矛盾するから $a \nmid m$ なので $a \in (\mathbb{Z}/n\mathbb{Z})^*$ この $a_\phi := a$ を取れば

$$\begin{aligned} \mathrm{Aut}(\mu_n) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \phi &\longmapsto a_\phi \end{aligned}$$

とできてこの a で ϕ が一意に定まるから全単射である。$\phi \circ \varphi(\zeta) = \phi(\zeta^{a_\varphi}) = (\zeta^{a_\varphi})^{a_\phi} = \zeta^{a_\varphi + a_\phi}$ と $\phi(\zeta) = \zeta^{a_\phi}, \varphi(\zeta) = \zeta^{a_\varphi}$ より準同型になるので $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ が成立する。 □

命題 12.27. K_n を K の n 分拡大とすると Rem (12.22) から K_n/K は Galois なので $G_n := \mathrm{Aut}_K(K_n) =$

$\mathrm{Gal}(K_n/K)$ とする。ζ を原始 n 乗根とし、 $\sigma \in G_n$ に対して $\sigma(\zeta) = \zeta^{a_\sigma}$ となる $a_\sigma \in \mathbb{Z}^+$ をとる。このとき

$$\begin{aligned} \chi_n : G_n &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* (\cong \mathrm{Aut}(\mu_n)) \\ \sigma &\longmapsto a_\sigma \end{aligned}$$

は単射群準同型となる。この χ_n をn 次円分指標 (cyclotomic character)といい Galois 表現の一種である。

Proof. $\sigma \in G_n$ に対して補題 (12.26) と同様に $\sigma(\zeta) = \zeta^{a_\sigma}$ で一意に定まるから χ_n は単射群準同型である。$^\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$ に対して $\phi(\zeta) = \zeta^a$ は K を固定するとは限らないので全射にはならない。 □

定義 12.28. $K = \mathbb{Q}$ のとき、その代数閉包を $\overline{\mathbb{Q}}$ としてその中で考える。

$$\begin{aligned} \Phi_n(X) &:= \prod_{\zeta:1 \text{ の原始 } n \text{ 乗根}} (X - \zeta) \\ &= (\zeta \text{の } \mathbb{Q} \text{ 上の最小多項式}) \\ &= (X^n - 1 \text{ の既約成分で}\zeta\text{を根に持つもの}) \end{aligned}$$

としてこの $\Phi_n(X)$ を第 n 次円分多項式 (cyclotomic polynomial)という。このとき $X^n - 1 = \prod_{d|n} \Phi_d(X)$ と $\deg(\Phi_n = \varphi(n)$ が成り立つ。ただしここで $\varphi(n)$ は Euler の関数であって $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ を満たす。

定理 12.29. (Gauss)

n 次円分多項式 Φ_n と n 次円分指標 χ_n で次が成り立つ。

(1) Φ_n は $\mathbb{Q}[X]$ において既約。

(2) $\chi_n : \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ は同型でとくに $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \phi(n) (= |(\mathbb{Z}/n\mathbb{Z})^*|)$ となる。

Rem 12.30. $\mathbb{Q}(\mu_\infty) := \mathbb{Q}(1 \text{ の任意の冪根})$ を全円分体という。このとき

$$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^* \cong \hat{\mathbb{Z}}^\times$$

となる。

Rem 12.31. Kronecker-weber の定理

$\mathbb{Q}$ の任意の Abel 拡大は $\mathbb{Q}(\mu_\infty)$ に含まれる。つまり、$\mathbb{Q}(\mu_\infty)$ は $\mathbb{Q}$ の最大 Abel 拡大であり $\mathbb{Q}^{\mathrm{ab}}$ とも書く。

$K = \mathbb{Q}(\sqrt{-m})$ の場合の最大 Abel 拡大は Kronecker の青春の夢と呼ばれていてそれ以外の場合は Hilbert の 12th problem として上がっている。

12.7 Kummer 拡大

以下では $n \in \mathbb{Z}^+$ と K : 体とする。ただし K は K の代数閉包におけるある 1 の原始 n 乗根 ζ を含んでいるとする。とくに $\mathrm{char}(K) = p > 0$ のときは $p \nmid n$ とする。

定義 12.32. 群 G がn で零化される (annihilated by n)とは $^\forall g \in G, g^n = e$ となること。

定義 12.33. 拡大 L/K が冪数 (定義 (12.12)) が n を割り切る Abel 拡大 (abelian of exponent dividing n) とはこの拡大が Abel 拡大でその Galois 群 $\mathrm{Gal}(L/K)$ が n で零化されること。冪数は元の位数の最小公倍数であったので任意の元は冪数乗すると単位元になるため n で零化されるときその冪数は文字通り n を割り切っている。

命題 12.34. $a \in K^\times$ に対して $X^n - a$ の K の代数閉包に入っているある根を $x := \sqrt[n]{a}$ とする。このとき他の根は $x\zeta^i$ $(1 \leq i \leq n-1)$ であり、$L = K(x)$ は $X^n - a$ の最小分解体で L/K が冪数が n を割り切る Abel 拡大となる。このような拡大 L/K を Kummer 拡大という。

Proof. 仮定より $\zeta \in K$ なので $X^n - a$ のすべての根は $L = K(x)$ に含まれるので $X^n - a$ の最小分解体になっている。$X^n - a$ のすべての根は $x\zeta^i$ で書かれるので重根を持たないから $X^n - a$ は分離多項式である。したがって定義 (12.2) より L/K は有限次 Galois 拡大である。

冪数が n を割り切ることを示す。$^\forall\sigma \in G := \mathrm{Gal}(L/K)$ をとる。σ は準同型であることと $\sigma|_K = \mathrm{id}_K$ であり、$a \in K^\times$ から $\sigma(x)^n = \sigma(x^n) = \sigma(a) = a$ となる。したがって $\sigma(x)$ も $X^n - a$ の根だから $\sigma(x) = x\zeta^i$ となる整数 $1 \leq i \leq n$ が存在する。よって合成写像 σ^n を考えると $\zeta \in K$ より $\zeta^i \in K$ だから

$$\begin{aligned}\sigma^n(x) &= \sigma^{n-1} \circ \sigma(x) \\ &= \sigma^{n-1}(x\zeta^i) \\ &= \sigma^{n-1}(x)\dot{\sigma}^{n-1}(\zeta^i) \\ &= \zeta^i\sigma^{n-1}(x) \\ &\vdots \\ &= (\zeta^i)^n x = x\end{aligned}$$

なので $\sigma^n(x) = x$ である。$\sigma|_K = \mathrm{id}_K$ だから $\sigma^n|_K = \mathrm{id}_K$ なので $\sigma^n = \mathrm{id}_L$ より定義 (12.32) から G は n で零化される。

G が Abel であることを示す。$\sigma, \sigma' \in G$ をとる。上記と同様に $\sigma(x) = x\zeta^i, \sigma'(x) = x\zeta^j$ となる i, j が存在する。K 上ではともに恒等写像だから $\sigma\sigma'|_K = \sigma'\sigma|_K$ である。また、$\sigma\sigma'(x) = \sigma(x\zeta^j) = \sigma(x)\sigma(\zeta^j) = x\zeta^i\zeta^j = x\zeta^{i+j}$ と $\sigma'\sigma(x) = \sigma'(x\zeta^i) = \sigma'(x)\sigma'(\zeta^i) = x\zeta^j\zeta^i = x\zeta^{j+i} = x\zeta^{i+j}$ より $\sigma\sigma'(x) = \sigma'\sigma(x)$ より $\sigma\sigma' = \sigma'\sigma$ なので Abel である。 □

命題 12.35. 命題 (12.34) の記号を用いる。$\mu_n := \{1 \text{ の } n \text{ 乗根} \in \overline{K}\}$ としたとき

$$\begin{aligned}\chi_a : G &\longrightarrow \mu_n \\ \sigma &\longmapsto \zeta^i\end{aligned}$$

は単射群準同型である。ただし $\sigma(x) = \zeta^i x$ を満たしている。よって補題 (12.25) から G は $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ の部分群に同型である。

Proof. $\sigma = \tau$ のとき写像として同じなので $\sigma(x) = x\zeta^i = \tau(x)$ より χ_a は写像になっている。$\chi_a(\sigma) = 1 = \zeta^0$ のとき $\sigma(x) = x\dot{1} = x$ より $\sigma = \mathrm{id}_K$ なので χ_a は単射。$\sigma, \tau \in G$ について $\sigma(x) = x\zeta^i, \tau(x) = x\zeta^j$ とすると $\zeta \in K$ から $\sigma\tau(x) = \sigma(x\zeta^j) = \sigma(x)\sigma(\zeta^j) = x\zeta^i\zeta^j = x\zeta^{i+j}$ より $\chi_a(\sigma\tau) = \zeta^{i+j}$ と $\chi_a(\sigma)\chi_n(\tau) = \zeta^i\zeta^j = \zeta^{i+j}$ より χ_a は単射準同型。 □

系 12.36. a が $K^\times$ で n の任意の約数 d において d 乗元でないとする。つまり剰余体 $K^\times/(K^\times)^n$ において a の像の位数が n であるとする。このとき $\chi_a : G \longrightarrow \mu_n$ は同型になる。

Proof. 命題 (12.35) より χ_a は単射準同型なのである μ_n の部分群と同型である。$\mathrm{Im}(\chi_a) \subset \mu_n$ で μ_n の部分群は Lagrange の定理から n のある約数 m を位数で持つから $\chi_a \cong \mu_m$ となる。$f := \prod_{\gamma\in\mu_m}(X - \gamma x) \in L[X]$ に任意の $\sigma \in G$ を作用させると $\sigma f = \prod_{\gamma\in\mu_m}(X - \sigma(\gamma x))$ となって $\gamma \in K$ より $\sigma(x) = \gamma' x, \gamma' \in \mu_m$

に対して $\sigma(\gamma x) = \sigma(\gamma)\sigma(x) = \gamma\gamma' x$ となる。そして μ_m は有限群だから γ が全体を動くとき $\gamma\gamma'$ も全体を動くので $\sigma f = f$ となる。任意の G の元で固定されるから L/K が Galois より $f \in K[X]$ である。また、$(\gamma x)^m = \gamma^m x^m = x^m$ より γx は x^m の m 乗根である。また、ある原始 m 乗根の冪も μ_m に含まれるので $|\mu_m| = m$ から $\deg(f) = m$ だから $X^m - x^m$ の K の代数閉包での根はすべて γx で書けるから $f = X^m - x^m$ となる。$f \in K[X]$ より $x^m \in K^\times$ である。$a^m = (x^n)^m = (x^m)^n \in (K^\times)^n$ だから a の $(K^\times)/(K^\times)^n$ への像の位数が n であることより $n \leq m$ を満たす。$m|n$ より $m \leq n$ でもあるから $n = m$ より $\mu_m = \mu_n$ である。したがって $G \cong \mu_m = \mu_n$ より χ_a は同型写像。 □

定理 12.37. Hilberts Satz 90

L/K が n 次巡回拡大のとき $\mathrm{Gal}(L/K)$ の生成元を σ とすると $\mathrm{N}_{L/K}(a) = 1$ となる $a \in L$ について $a = \sigma(b)/b$ となる $b \in L$ が存在する。

定理 12.38. K の n 次巡回拡大 L はある $a \in (K^\times \cap (L^\times)^n)/(K^\times)^n$ により $L = K(\sqrt[n]{a})$ と書ける。

Proof. L/K は n 次巡回拡大なので $G := \mathrm{Gal}(L/K)$ としたとき G は位数 n の巡回群だから $\chi : G \longrightarrow \mu_n$ が同型となる χ が存在する。G の生成元を σ とすると $\chi(\sigma) \in \mu_n \subset K$ だから例 (**??**) より $\mathrm{N}_{L/K}(\chi(\sigma)) = (\chi(\sigma))^n = 1$ なので Hilberts Satz 90 (12.37) より $\chi(\sigma) = \sigma(\theta)/\theta$ となる $\theta \in L^\times$ が存在する。$(\chi(\sigma))^n = 1$ より $\sigma(\theta)^n/\theta^n = 1$ なので $\sigma(\theta^n) = \theta^n$ より θ^n は G の生成元で固定されるため、G の任意の元で固定されるから L/K が Galois より $\theta^n \in K^\times$ となるから $a := \theta^n$ とおく。$\theta \in L^\times$ より $a = \theta^n \in (L^\times)^n$ でもあるから $a \in K^\times \cap (L^\times)^n$ である。a は任意の θ^n の n 乗根をとっていいからそれをまとめて書くために $a \in K^\times \cap (L^\times)^n/(K^\times)^n$ として a を取り直す。

$f \in K[X]$ を θ の最小多項式とする。このとき $\chi(\sigma) \in \mu_n$ から $\chi(\sigma) = \zeta^j$ とおくと $1 \leq i \leq n$ で $\sigma^i(\theta) = \sigma^{i-1}(\zeta^j\theta) = \cdots = (\zeta^j)^i\theta$ となる。$(\sigma^i(\theta))^n = (\zeta^{i+j}\theta)^n = \theta^n = a$ より $\sigma^i(\theta)$ も $X^n - a \in K[X]$ の根である。$\sigma^i \in G$ より $f(\sigma^i(\theta)) = \sigma^i(f(\theta)) = 0$ だから $\sigma^i(\theta)$ は θ と同じ最小多項式を持つ。したがって θ を根にもつ $X^n - a$ は $\zeta^{i+j}\theta$ の n 根をもち、これ以上次数が下がらないので $f = X^n - a$ である。そして $\theta \in L$ と $\zeta \in K$ なので $\zeta^{i+j}\theta \in L$ だから f は $L[X]$ で一次の積に分解されてその根はすべて異なるから分離的である。$[K(\theta) : K] = \deg(f) = n = [L : K]$ で $K(\theta) \subset L$ より $L = K(\theta) = K(\sqrt[n]{a})$ なので示された。 □

Fact 12.39. より一般に L/K を K の冪数が n を割り切る最大 Abel 拡大とすると

$$\begin{aligned} \mathrm{Gal}(L/K) \times K^\times/(K^\times)^n &\longrightarrow \mu_n \\ (\sigma, a) &\longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{aligned}$$

は双線形で一意に定まる。これより $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(K^\times/(K^\times)^n, \mu_n)$ も従う。

12.8 Artin-Schreier 拡大

以下では $\mathrm{char}(K) = p > 0$ とする。 $(\Leftrightarrow K \supset \mathbb{F}_p)$

命題 12.40. K の代数閉包 Ω 上で以下のように対応を定める。

$$\begin{aligned} \mathscr{P} : \Omega &\longrightarrow \Omega \\ x &\longmapsto x^p - x \end{aligned}$$

するとこれは Ω の加法群の準同型になり、とくに $\mathscr{P}|_K$ は K の加法群の準同型になる。その核は $\mathbb{F}_p$ である。

Proof. $x = y$ のとき明らかに $x^p - x = y^p - y$ より $\mathscr{P}$ は写像。$\mathscr{P}(x+y) = (x+y)^p - (x+y) = x^p + y^p - x - y = (x^p - x) + (y^p - y) = \mathscr{P}(x) + \mathscr{P}(y)$ より加法群の準同型。また、 $\mathbb{F}_p \subset K \subset \Omega$ で系 (12.15) から Ω のなかで $\mathbb{F}_p = \{x \in \Omega | x^p = x\}$ と書けるから $\mathscr{P}(x) = 0 \Leftrightarrow x^p - x = 0 \Leftrightarrow x^p = x \Leftrightarrow x \in \mathbb{F}_p$ より $\ker(\mathscr{P}) = \mathbb{F}_p$ となる。$\mathbb{F}_p \subset K$ なので $\ker(\mathscr{P}|_K) = \mathbb{F}_p$ にもなる。 □

補題 12.41. $a \in K$ に対して $f := X^p - x - a \in K[X]$ とおいてそのある根を $x \in \Omega$ とおく。このとき f が K 上で可約であることと $a \in \mathscr{P}(K)$ は必要十分である。

Proof. $a \in \mathscr{P}(K) \Leftrightarrow {}^{\exists}\alpha \in K, \alpha^p - \alpha = a = x^p - x$ から $\mathrm{char}(K) = p > 0$ より $(x-\alpha)^p = x - \alpha$ なので $\mathbb{F}_p = \{x \in \Omega | x^p = x\}$ から $x - \alpha \in \mathbb{F}_p \subset K$ である。$\alpha \in K$ より $(x-\alpha) + \alpha = x \in K$ となる。また、$x \in K$ のとき $x^p - x - a = 0 \Leftrightarrow a = x^p - x$ より $a \in \mathscr{P}(K)$ となる。したがって $a \in \mathscr{P}(K) \Leftrightarrow x \in K$ が成り立つので f が K 上可約 $\Leftrightarrow x \in K$ を示せば良い。

$g(X) \in K[X]$ を x の K 上の最小多項式とすると $f(x) = 0$ と $\deg(g)$ の最小生から $g(X)|f(X)$ である。$f(X) = X^p - X - a$ はその形から $f(X) = f(X+1)$ なので $f(X) = f(X+1) = \cdots = f(X+i) = \cdots = f(X+(p-1)), i \in \mathbb{F}_p$ となっている。f が p 次であることと ${}^{\forall}i \in F_p$ に対して $0 = f(x) = f(x+i)$ より $x+i$ も f の根になっているから f の根はすべて $x+i$ の形で書ける。

ここで $g(X) = g(X+1)$ のとき同様に $g(X) = g(X+1) = \cdots = g(X+i) = \cdots = g(X+(p-1))$ である。$g(X)$ は x を根に持っていたから $0 = g(x) = g(x+i)$ より $x+i$ も $g(X)$ の根になるので少なくとも p 個の相異なる根を持っていて $g|f$ から $\deg(g) \leq p$ なので $\deg(g) = p$ となり、$g(X) = \prod_{i=0}^{p-1}(X - (x+i))$ と書ける。f の根もすべて $x+i$ であるから $g = f$ となる。したがって g が最小多項式なので f は既約。対偶をとって f が可約 $\Rightarrow g(X) \neq g(X+1)$ が言えた。

$g(X) \neq g(X+1)$ のときある $k \in \mathbb{F}_p$ で $g(X) = g(X+k)$ となったとする。このとき $0 \leq l \leq p-1$ で $g(X) = g(X+k) = g(X+2k) = \cdots = g(X+lk) = \cdots = g(X+(p-1)k)$ となる。lk は l によってそれぞれ異なり、それが p 個あるのである l で $g(X+1) = g(X+lk)$ となるものが存在する。これは $g(X) \neq g(X+1)(= g(X+lk))$ に矛盾するので $g(X), g(X+1), \ldots, g(X+(p-1))$ は相異なる。$g(X)|f(X)$ から任意の $i \in \mathbb{F}_p$ で $g(X+i)|f(X+i) = f(X)$ となるから $\prod_{i=0}^{p-1} g(X+i)|f(X)$ となり、 $g(X+i)$ がそれぞれ異なるから $f(X)$ は可約。したがって $g(X) \neq g(X+1) \Rightarrow f$ が可約が言えた。

とくにこのとき $\deg(f) = p$ なので $f = \prod_{i=0}^{p-1} g(X+i)$ で $g(X)$ は x の K 上の最小多項式であったから $\deg(g(X+i)) \leq 1$ だから $g(X+i)$ は一次式であり、$g(X) = X - x \in K[X]$ となる。よって $f = \prod_{i=0}^{p-1}(X-(x+i))$ と K 上で一次式の積に分解できて $x \in K$ となる。したがって $g(X) \neq g(X+1) \Rightarrow f$ が可約 $\Rightarrow f = \prod_{i=0}^{p-1}(X-(x+i))$ と分解できる $\Rightarrow x \in K$ が言えた。

$x \in K$ のとき $x+i \in K$ だから f は K 上で $f = \prod_{i=0}^{p-1}(X-(x+i))$ と分解できて x の最小多項式 $g \in K[X]$ は $g(X) = X - x$ となるから $g(X) \neq g(X+1)$ である。したがって逆も言えて f が可約 $\Leftrightarrow x \in K$ となるので $x \in K \Leftrightarrow a \in \mathscr{P}(K)$ より示された。 □

命題 12.42. ある $a \in K$ に対して $\mathscr{P}(x) = a$ となる $x \in \Omega$ をとる。このとき $L := K(x)$ とすると L/K は冪数が n を割り切る Abel 拡大であり、$G := \mathrm{Gal}(L/K)$ とおいたとき加法群としての $\mathbb{F}_p$ に対して

$$\begin{aligned} \chi_a : G &\longrightarrow \mathbb{F}_p \\ \sigma &\longmapsto \sigma(x) - x \end{aligned}$$

という単射群準同型が存在する。とくに $a \in K - \mathscr{P}(K) = K - \mathrm{Im}(\mathscr{P})$ を取ったときは χ_a は全射になり、L/K は p 次巡回拡大になる。このような拡大 L/K を Artin-Shreier 拡大という。

Proof. $\mathscr{P}(x)=a$ となる x は $\mathscr{P}(x)=x^p-x=a$ より $f:=X^p-X-a\in K[X]$ の根になっている。ここで $x+i, i\in\mathbb{F}_p$ は $\mathbb{F}_p=\{x\in\Omega|x^p=x\}$ と $\mathrm{char}(K)=p>0$ なので $(x+i)^p-(x+i)-a=x^p+i^p-x-i-a=x^p-x-a=0$ より f の根になる。$1\leq i\leq p$ だから f の根はこれで全てなので $\mathbb{F}_p\subset K$ より L は f の最小分解体であり、全て根が異なるから分離多項式なので L/K は p 次 Galois 拡大となる。

$f(\sigma(x))=(\sigma(x))^p-\sigma(x)-a=\sigma(x^p-x-a)=0$ だから $\sigma(x)$ も f の根であるのである $i_\sigma\in\mathbb{F}_p$ で $\sigma(x)=x+i_\sigma$ となるから $\sigma(x)-x=i_\sigma\in\mathbb{F}_p$ となる。したがって χ_a の終域は確かに $\mathbb{F}_p$ になる。$\sigma=\tau\in G$ のとき $\sigma(x)-x=\tau(x)-x$ より χ_a は写像になっている。また、$\chi_a(\sigma)=0$ のとき $\sigma(x)-x=0\Leftrightarrow\sigma(x)=x$ より $\sigma=\mathrm{id}_L$ より χ_a は単射。$\chi_a(\sigma\circ\tau)=\sigma\circ\tau(x)-x=\sigma(x+i_\tau)-x=(x+i_\sigma)+i_\tau-x=i_\sigma+i_\tau$ であり、$\chi_a(\sigma)+\chi_a(\tau)=(\sigma(x)-x)+(\tau(x)-x)=i_\sigma+i_\tau$ より $\chi_a(\sigma\circ\tau)=\chi_a(\sigma)+\chi_a(\tau)$ だから χ_a は群準同型になる。

$^\forall\sigma\in G$ に対して $\mathrm{char}(K)=p>0$ から $\sigma^p(x)=\sigma^{p-1}(x+i)=\sigma^{p-1}(x)+\sigma^{p-1}(i)=\sigma^{p-1}(x)+i=\cdots=x+pi=x$ より $\sigma^p(x)=x$ となる。したがって $\sigma^n=\mathrm{id}_L$ より p で零化される。$\sigma\circ\tau(x)=\sigma(x+i_\tau)=x+i_\sigma+i_\tau$ と $\tau\circ\sigma(x)=\tau(x+i_\sigma)=x+i_\tau+i_\sigma$ で $i_\sigma+i_\tau=i_\tau+i_\sigma$ より $\sigma\circ\tau=\tau\circ\sigma$ なので G は可換だから L/K は冪数が p を割り切る Abel 拡大。p が素数より冪数が 1 か p だから G は単位元のみの位数 1 の群になるか位数 p の元を持つ巡回群になるかである。

$a\in K-\mathscr{P}(K)$ を取ったとき補題 (12.41) の否定から $f=X^p-X-a$ は既約で f は x の最小多項式である。L/K は Galois より $|G|=[L:K]=\deg(f)=p=|\,\mathbb{F}_p\,|$ である。χ_a が単射なので $|G|=|\,\mathbb{F}_p\,|$ より全射になるから χ_a は同型になる。$\mathbb{F}_p$ は加法群として巡回群なので L/K は p 次の巡回拡大になる。 □

定理 12.43. $\mathbb{F}_p$ を含む体 K の p 次巡回拡大はすべて命題 (12.42) のようにして作られる。

Fact 12.44. $\mathbb{F}_p$ を含む体 K について $p\nmid n$ となる n 次巡回拡大は定理 (12.38) のようにして、p 次巡回拡大は定理 (12.43) のようにして作られる。p の冪次については K の加法群の代わりに Witt ベクトルの群を考える Artin-Shreier-Witt 理論を用いて作られる。