数理解析研究所講究録
997 巻 1997 年 58-65

標数 2 の曲線の $(2,2)$-Galois 被覆の持ち上げについて

中央大学理工学研究科　伊藤崇史（TAKASHI ITO）

0 introduction

$k:\mathrm{ch}\,(k)=p(>0)$ なる代数閉体、$A(\succ W(k)[\zeta_p])$:離散附値環、$K:Q(A)$（$W(k)$ は k の Witt 環、ζ_p は 1 の原始 p 乗根、Q は商体）とする。k 上の曲線の被覆の持ち上げとは、混標数の離散附値環 $(A,\mathfrak{M})$ 上の曲線の $\otimes_A k$ 上で退化しない被覆のことです。

k 上の曲線の p 次巡回被覆は Artin-Schreier 拡大で記述され、K 上の曲線の p 次巡回拡大は Kummer 拡大で記述されます。したがって、A 上の曲線の p 次巡回拡大は Artin-Schreier 系列から Kummer 系列への変形で与えられるはずです。そして実際、乗法群スキームから加法群スキームへの変形を司る群スキーム $\mathcal{G}^{(\lambda)}=\mathrm{Spec}\,A[X,\frac{1}{\lambda X+1}]$（$\lambda=\zeta_p-1$）によってそれは実現されています。[2]

この p 次巡回拡大の持ち上げを組み合わせて、$\mathbf{P}_k^1$ の一点の上で wild に分岐し Galois 群が $\mathbf{Z}/p\times\mathbf{Z}/p$ となる場合について持ち上げが構成できるか計算してみました。
(p,p)-covering $C\to\mathbf{P}_k^1$ に対応する曲線 C の関数体は $k(C)=k(x,y)/(y^{p^2}-y-f(x))$ と言う形に書けます。C が $\mathbf{P}_k^1$ 上で分岐点を一個だけ持つ場合を考えるので $f(x)=\dfrac{\text{高々 } e \text{ 次の多項式}}{x^e}$（$p\nmid e$）という形のものについて計算すれば十分です。$k(C)$ を二つの p 次巡回拡大 $k(C_1)=k(x,U)/(U^p-U-f_1(x))$ と $k(C_2)=k(x,V)/(V^p-V-f_2(x))$ の合成と思うと、対応する p-covering 曲線 C_1, C_2 によって $C=C_1\times_{\mathbf{P}_k^1}C_2$ となります。p 次巡回拡大の持ち上げ $\tilde{C}_1,\tilde{C}_2$ に対して、$\tilde{C}:=\tilde{C}_1\times_{\mathbf{P}_K^1}\tilde{C}_2$ と置いて genus $g(C)=g(\tilde{C})$ となっていれば (p,p)-covering の持ち上げが作れたことになります。

以後 $p=2$ とします。そうすると $e=2r+1$ と書けます。$g(C)=g(\tilde{C})$ となるためには、C_1,C_2 の持ち上げ $\tilde{C}_1,\tilde{C}_2$ の分岐点が $r+1$ 点重なっていることが必要です（種数の計算より）。C_i の自然な持ち上げ $\tilde{C}_i$ の式は $Y^2=\dfrac{e\text{ 次式}}{X^e}$ と書けます。ここで $X=0$ という分岐点は $\tilde{C}_1,\tilde{C}_2$ の両方に共通ですが、分子の方は全然共通解が無いことが附値の計算で確かめることができて、C_i の自然な持ち上げでは $\tilde{C}$ は C の持ち上げにはなっていませ

ん。C_1 はそのままで、C_2 は別の持ち上げを取ることを考えます。右辺の分母 X^{2r+1} を、$X(X-\gamma_1)^2\dots(X-\gamma_r)^2$ （γ_i は $\mathfrak{M}$ の元）と取り替え、適当な γ_i を取ることで C_1 の分岐点と r 個よけいに重ねられれば良いのです。そしてそのような γ_i についての連立方程式の解が本当に在って、$\mathfrak{M}$ に入っていることを確かめることが出来ました。

1 必要な準備

k, A, Kを intro のとおり、$\lambda=\zeta_p-1$ としたとき A 上の scheme の巡回 covering は次の abelian sheaf によって支配されている。[2]

$$\begin{array}{ccccccccc} 0 & \to & (\mathbf{Z}/p)_A & \to & \mathcal{G}^{(\lambda)} & \to & \mathcal{G}^{(\lambda^p)} & \to & 0 \\ & & & & x & \mapsto & \frac{1}{\lambda^p}((1+\lambda x)^p-1) & & \end{array}$$

$\mathcal{G}^{(\lambda)}=\operatorname{Spec}A[X,\frac{1}{1+\lambda X}]$ であり、$x\mapsto 1+\lambda x$ によって $\mathbf{G}_{m,K}\xrightarrow{\sim}\mathcal{G}^{(\lambda)}\underset{A}{\otimes}K$ が、また $\mathcal{G}^{(\lambda)}\underset{A}{\otimes}k=\mathbf{G}_{a,k}$ が得られる。さらに、$\frac{1}{\lambda^p}((1+\lambda x)^p-1)$ を展開して mod λ すると Artin-Schreier 理論でおなじみの $(\text{Frobenius}-1)(x)=x^p-x$ になる。

一般に離散附値環 $(A,\mathcal{M})$ 上の群 scheme で、special fibre 上で加法群 scheme となって generic fibre 上で乗法群 scheme となるのは $\mathcal{G}^{(a)}$, $a\in\mathcal{M}$ という群 scheme に限る。[1]

Artin-Schreier 拡大の標数 0 の Kummer 拡大への変形は $\mathcal{G}^{(\lambda)}$ の演算を用いて実行できる。

$$D/k:\text{algebraic curve},\ k(C)/k(D):\text{Artin-Schreier 拡大}$$

$\exists y\in k(C)$, $\exists f\in k(D)$ s.t. $y^p-y=f$. $y^p-y=f$ を $\frac{1}{\lambda^p}((1+\lambda y)^p-1)=\tilde{f}$ で置き換えれば（$\tilde{f}$ は mod λ で f になる適当な持ち上げ）D の model $\tilde{D}$ の p 次 Kummer covering が得られる。

$$Y=1+\lambda y \text{ として } K(\tilde{D})(Y) \text{ s.t. } Y^p=1+\lambda^p\tilde{f}.$$

k 上の曲線 D の (p,p)-covering 曲線 C は $k(C)=k(D)(y)$ s.t. $y^{p^2}-y\in k(D)$ という形の標準型を持つ（一般に $q=p^n$, $\mathbf{F}_q$ を含む体の $(\mathbf{Z}/p)^n$ 拡大について同様のことが言える）。$D=\mathbf{P}^1_k$ とし Riemann-Hurwitz の定理により

$$2g(C)-2=-2p^2+\sum_{Q\in C}\operatorname{length}(\Omega_{C/\mathbf{P}^1_k})_Q.$$

$y^{p^2}-y=f$ の右辺の有理関数 f を

$$f(x)=\frac{h(x)}{(x-\alpha_1)^{e_1}\cdots(x-\alpha_r)^{e_r}}$$

$$\deg(h(x)) \le \sum_i e_i,\ (p, e_i) = 1$$

なる場合 length $\Omega_{C/\mathbf{P}^1_k}$ を計算すると、

$$g(C) = 1 - p^2 + \frac{p^2-1}{2}\sum_i (e_i + 1).$$

2 (p,p) 拡大の変形の一般論

$\mathbf{F}_{p^2} = \mathbf{F}_p \oplus \mathbf{F}_p\xi$ と書くことにする。関数体 K の (p,p) 拡大 L は $\exists Y \in L$, $L = K(Y)$ s.t. $\exists f \in K$, $Y^{p^2} - Y - f = 0$ と標準化することができる。これを K の Artin-Schreier 拡大 $K(U)$, $K(V)$ の合成の形に分解する。

L に対する $\mathbf{P}^1$ の (p,p) covering 曲線 C と部分体 $K(U)$, $K(V)$ に対応する曲線を C_1, C_2 とする。

$C: y^{p^2} - y = \frac{f(x)}{x^e}$, $f(x) \in k[x]$ の場合で、さらに話を簡単にするため $p \nmid e$ に限って話をする。そうすると

$$\begin{cases} C_1 : U^p - U + \frac{1}{\xi^p - \xi}\frac{f(x)}{x^e} = 0 \\ C_2 : V^p - V + \frac{\xi^p}{\xi^p - \xi}\frac{f(x)}{x^e} = 0 \end{cases}$$

と書けることが簡単な計算で分かる。

C の種数は Rieman-Hurwitz の公式より $2g(C) - 2 = p^2(-2) + (e+1)(p^2-1)$ を満たす。C_i の種数は $2g(C_i) - 2 = p(-2) + (e+1)(p-1)$ を満たす。Artin-Schreier to Kummer により $\tilde{U} = 1+\lambda U$, $\tilde{V} = 1+\lambda V$, $\tilde{W} = 1+\lambda W$ とおき、適当な model を取ることで $\tilde{U}^p$, $\tilde{V}^p$ の分子が各々重根を持たないようにすれば $2g(\tilde{C}_i) - 2 = p(-2) + (e+1)(p-1)$ なので確かに C_i の持ち上げになっている。

曲線 $\tilde{C}$ を関数体 $Q(A)(x, \tilde{U}, \tilde{V})$ に対応した曲線とする。$\tilde{C}_1$ と $\tilde{C}_2$ の分岐点が右辺の分母から定まる分岐点以外で重ならないと

$$2g(\tilde{C}) - 2 = p^2(-2) + p(2e+1)(p-1)$$

となるので C の種数と一致しない。右辺の持ち上げ適当に取って、分子から来る分岐点を n 個重ねることが出来れば

$$2g(\tilde{C}) - 2 = p^2(-2) + p(2e-n+1)(p-1)$$

となり、$\tilde{C}$ が持ち上げになっているためには

$$p(p-1)(2e-n+1) = (p^2-1)(e+1)$$

でなければならない。

$$\therefore p \mid (p+1)(e+1)$$

即ち $p \mid e+1$ が必要条件。

$e=pr+p-1$ としたときには $n=(r+1)(p-1)-1$ 個の分岐点を重ねなくてはならない。

3 $(2,2)$ 拡大の変形の存在

関数体 $k(x,y)$ を持つ $\mathbf{P}^1$ の $(2,2)$ 被覆曲線

$$C : y^4 - y = \frac{f(x)}{x^{2n+1}},\ f(x) = a_0 + a_1 x + \ldots + a_{2n+1}x^{2n+1},\ a_i \in k,\ a_0 \neq 0$$

が一般に標数 0 に持ち上げ可能であることを示す。これは前節の議論より Artin-Schreier 被覆の合成に分解しておいて、右辺の持ち上げを適当に取ることでそれぞれの中間体の分子から定まる分岐点を n 個重ねられることを示せば良い。

巡回拡大に分解すれば $k(x,y)=k(x,U,V)$

$$\begin{cases} C_1 : U^2 - U = \dfrac{f(x)}{x^{2n+1}} \\ C_2 : V^2 - V = \xi^2 \dfrac{f(x)}{x^{2n+1}}, \quad \xi^2+\xi+1=0 \end{cases}$$

である。$f(x)$ や ξ などの A における代表元を固定し、誤解のおそれはないと思われるので A 上でも同じ記号を使う。$W(k)$ の指数付値の A における拡張 v_A を $v_A(2)=1$ となるように定める。

Artin-Schreier to Kummer によって、

$$\begin{cases} \tilde{C}_1 : \tilde{U}^2 = 1 + 4\dfrac{f(x)}{x^{2n+1}} = \dfrac{1+4a_{2n+1}}{x^{2n+1}}(x-\alpha_1)\cdots(x-\alpha_{2n+1}) \\ \tilde{C}_2 : \tilde{V}^2 = 1 + 4\xi^2\dfrac{f(x)}{x^{2n+1}} = \dfrac{1+4\xi^2 a_{2n+1}}{x^{2n+1}}(x-\beta_1)\cdots(x-\beta_{2n+1}) \end{cases}$$

と右辺の持ち上げを素直に取る場合を考える。$f(0)=a_0\neq 0$ 故 $\alpha_i \neq 0, \beta_i \neq 0\,(\forall i)$ で、α_i, β_i は A の元であることに注意する。

β_i を $(1+4a_{2n+1})(x-\alpha_1)\cdots(x-\alpha_{2n+1})$ に代入すると、

$$\begin{aligned} & (1+4a_{2n+1})(\beta_i-\alpha_1)\cdots(\beta_i-\alpha_{2n+1}) \\ = \ & {\beta_i}^{2n+1} + 4f(\beta_i) = {\beta_i}^{2n+1} + 4\xi^2 f(\beta_i) - 4\xi^2 f(\beta_i) + 4f(\beta_i) \\ = \ & 4f(\beta_i)(1-\xi^2) \neq 0 \end{aligned}$$

よって共通解はない。

${\alpha_i}^{2n+1} = -4f(\alpha_i)$ の両辺に v_A を作用させて

$$(2n+1)v_A(\alpha_i) = 2 + v_A(f(\alpha_i))$$

$v_A(f(\alpha_i)) = v_A(a_0) = 0$ となるから

$$\therefore v_A(\alpha_i) = \frac{2}{2n+1}\text{、同様に } v_A(\beta_i) = \frac{2}{2n+1}.$$

また $(1+4a_{2n+1})(\beta_i-\alpha_1)\cdots(\beta_i-\alpha_{2n+1})=4f(\beta_i)(1-\xi^2)$ の両辺に v_A を作用させると

$$v_A(\beta_i-\alpha_1)+\cdots+v_A(\beta_i-\alpha_{2n+1})=2.$$

$v_A(\beta_i-\alpha_j)\geq\frac{2}{2n+1}$ であったことを思い出すと、

$$v_A(\beta_i-\alpha_j)=\frac{2}{2n+1}\quad 1\leq\forall i,j\leq 2n+1\,.$$

α_i が $x^{2n+1}+4f(x)$ の重根だとすると $\deg f\geq 1\,(\because \alpha_i\neq 0)$ で $(x^{2n+1}+4f(x))'=(2n+1)x^{2n}+4f'(x)$ の根である。$(2n+1){\alpha_i}^{2n}=-4f'(\alpha_i)$ に v_A を作用させると

$$2nv_A(\alpha_i)=2+v_A(a_1+\cdots+(2n+1)a_{2n+1}{\alpha_i}^{2n})$$

故に $\frac{4n}{2n+1}=2+(j-1)\frac{2}{2n+1}+v_A(j)$ ただし j は $a_j\neq 0$ となる最小の数。よってこのような正整数は存在しないので矛盾。同様に $x^{2n+1}+4\xi^2 f(x)$ も重根を持たない。

以上で $\tilde{C}_1$ と $\tilde{C}_2$ が各々C_1 と C_2 の lifting で、$\tilde{C}_1$ と $\tilde{C}_2$ の分岐点は分母以外では重なっていないことが示された。従ってこのままでは $n\gneq 0$ の時 $Q(A)(x,\tilde{U},\tilde{V})$ は C の lifting とはならない。

<u>**Lemma**</u> $1\leq\forall i,j\leq 2n+1,\ i\neq j$ ならば $v_A(\beta_i-\beta_j)=\frac{2}{2n+1}$。
Proof

$$\begin{aligned}&(x^{2n+1}+4\xi^2 f(x))'=(2n+1)x^{2n}+4\xi^2 f'(x)\\ =\ &(1+4\xi^2)\{(x-\beta_2)\cdots(x-\beta_{2n+1})+\cdots+(x-\beta_1)\cdots(x-\beta_{2n})\}\end{aligned}$$

に β_i を代入すると

$$\begin{aligned}&(2n+1){\beta_i}^{2n}+4\xi^2 f(\beta_i)\\ =\ &(1+4\xi^2 a_{2n+1})(\beta_i-\beta_1)\cdots(\beta_i-\beta_{i-1})(\beta_i-\beta_{i+1})\cdots(\beta_i-\beta_{2n+1}).\end{aligned}$$

両辺に v_A を作用させると $v_A({\beta_i}^{2n})=\frac{4n}{2n+1}\lneq v_A(4\xi^2 f(\beta_i))=2.$ 従って

$$\frac{4n}{2n+1}=v_A(\beta_i-\beta_1)+\cdots+v_A(\beta_i-\beta_{2n+1}).$$

ところが $i\neq j$ ならば $v_A(\beta_i-\beta_j)\geq\frac{2}{2n+1}$ である。

$$\therefore v_A(\beta_i-\beta_j)=\frac{2}{2n+1}\quad(\forall i\neq j)\qquad\qquad \textbf{qed.}$$

以下では $n\gneq 0$ として、$\tilde{C}_1$ の別の lifting で $\tilde{C}_2$ の分岐点と n 個よけいに重なっているものを構成する。

$1+4\frac{f(x)}{x(x-\gamma_1)^2\cdots(x-\gamma_n)^2}$ なる式で $x(x-\gamma_1)^2\cdots(x-\gamma_n)^2+4f(x)$ が解 $\beta_1,\ldots,\beta_n$ を持つものを構成する。それが求める別の lifting となるのである。

$\gamma_1,\ldots,\gamma_n$ は n 個の超曲面

$$\begin{cases} \beta_1(\beta_1-X_1)^2\cdots(\beta_1-X_n)^2+4f(\beta_1)=0 \\ \vdots \\ \beta_n(\beta_n-X_1)^2\cdots(\beta_n-X_n)^2+4f(\beta_n)=0 \end{cases}$$

の交点と解釈できる。${\beta_i}^{2n+1}+4\xi^2 f(\beta_i)=0,\ \beta_i\neq 0$ より

$$\left\{(\beta_i-X_1)\cdots(\beta_i-X_n)-\frac{{\beta_i}^n}{\xi}\right\}\left\{(\beta_i-X_1)\cdots(\beta_i-X_n)+\frac{{\beta_i}^n}{\xi}\right\}=0$$

の交点である。まず

$$\begin{cases} (\beta_1-X_1)\cdots(\beta_1-X_n)-\dfrac{{\beta_1}^n}{\xi}=0 \\ \vdots \\ (\beta_n-X_1)\cdots(\beta_n-X_n)-\dfrac{{\beta_n}^n}{\xi}=0 \end{cases}$$

の交点について考察する。

$$S_1=(-1)(X_1+\cdots+X_n),\ldots,S_n=(-1)^n X_1\cdots X_n$$

を $X_1,\ldots,X_n$ の基本対称式 $\times(\pm 1)$ とする．上の連立方程式を、未知変数 $S_1,\ldots,S_n$ の連立一次方程式と考え直すと

$$\begin{pmatrix} {\beta_1}^{n-1} & \cdots & \beta_1 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ {\beta_n}^{n-1} & \cdots & \beta_n & 1 \end{pmatrix}\begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix}=\left(\frac{1}{\xi}-1\right)\begin{pmatrix} {\beta_1}^n \\ \vdots \\ {\beta_n}^n \end{pmatrix}$$

この行列の行列式は Vandermonde 行列式を転置したものである。従って -1 倍の不定さをのぞき $(\beta_1-\beta_2)(\beta_1-\beta_3)\cdots(\beta_{n-1}-\beta_n)$ に等しい．よって Lemma により正則行列であり、$(S_1,\ldots,S_n)$ は $Q(A)^n$ の元として unique に定まる。ここで多項式 $X^n+S_1X^{n-1}+\cdots+S_n$ を考える。$S_1,\ldots,S_n$ が基本対称式であったことを思い出すと

$$X^n+S_1X^{n-1}+\cdots+S_n=(X-X_1)\cdots(X-X_n)$$

である。よって A を十分大きくとれば $Q(A)^n$ の中で超曲面の交点が決まる。他の既約成分同士の交点は右辺のベクトルを他の適当な形に書き換えれば同様にうまくいく。故に $(\gamma_1,\ldots,\gamma_n)\in Q(A)^n$ は有限個しか存在しない。β_{n+1}

によって定まる超曲面がこの交点を通るとする。そうすると以下の連立方程式の解によって交点は定まる。

$$\begin{pmatrix} {\beta_1}^{n-1} & \dots & \beta_1 & 1 & (1\pm\frac{1}{\xi}){\beta_1}^n \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ {\beta_{n+1}}^{n-1} & \dots & \beta_{n+1} & 1 & (1\pm\frac{1}{\xi}){\beta_{n+1}}^n \end{pmatrix}\begin{pmatrix} S_1 \\ \vdots \\ S_n \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

(ここで ± は + または − の意味) .

従って、この行列の行列式は 0 でなければならない。

$$\begin{aligned} &\begin{vmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ {\beta_1}^{n-1} & \dots & {\beta_{n+1}}^{n-1} \\ \left(1\pm\frac{1}{\xi}\right){\beta_1}^n & \dots & \left(1\pm\frac{1}{\xi}\right){\beta_{n+1}}^n \end{vmatrix} \\ = &\left(1-\frac{1}{\xi}\right)\times(\ (n+1)\ \text{変数の Vandermonde 行列式}\ ) \\ + &\frac{2}{\xi}\sum_i(-1)^{n+1+i}\{{\beta_i}^n\times(\ n\ \text{変数の Vandermonde 行列式}\ )\} \end{aligned}$$

(i は ${\beta_i}^n$ に $1+\frac{1}{\xi}$ が掛かっているものについての和)

の右辺の各項に v_A を作用させると

$$\begin{aligned} &v_A\left(\left(1-\frac{1}{\xi}\right)\times(\ n+1\ \text{変数の Vandermonde 行列式}\ )\right) \\ = &\frac{(n+1)n}{2n+1}, \\ &v_A\left(\frac{2}{\xi}{\beta_i}^n\times(\ n\ \text{変数の Vandermonde 行列式}\ )\right) \\ = &1+\frac{2n}{2n+1}+\frac{n(n-1)}{2n+1}=1+\frac{(n+1)n}{2n+1}. \end{aligned}$$

従って、全体の付値の値は $\frac{(n+1)n}{2n+1}(<\infty)$ となって $\det\neq 0$。故に解を持たない。よって β_{n+1} の超曲面とは交わらない。この議論は β_i の取り方に依存していない。従って勝手な n 個の β_i の組についても有限個の交点しか存在せず、$n+1$ 個の組にたいしては交点は存在しない。

$$x(x-\gamma_1)^2\cdots(x-\gamma_n)^2+4f(x)=(1+4a_{2n+1})(x-\alpha'_1)\cdots(x-\alpha'_{2n+1})$$

$\alpha'_1=\beta_1,\dots,\alpha'_n=\beta_n$ とする。

$\beta_i(\beta_i-\gamma_1)^2\cdots(\beta_i-\gamma_n)^2=-4f(\beta_i)$ の両辺に v_A を作用させて

$$v_A(\beta_i-\gamma_1)+\cdots+v_A(\beta_i-\gamma_n)=\frac{2n}{2n+1}$$

を得る。以下、背理法により $\gamma_j \in \mathfrak{M}_A$ であることを示す。$\exists \gamma_j$ s.t. $v_A(\gamma_j) \lneq \frac{2}{2n+1}$ と仮定する。$v_A(\beta_i - \gamma_j) = v_A(\gamma_j)$ である。番号を付け替えて γ_j を γ_1 とする。すべての $v_A(\beta_1 - \gamma_j)$ が $\frac{2}{2n+1}$ より小さいということは有り得ないので $\exists \gamma_j$ s.t. $v_A(\beta_1 - \gamma_j) \gneq \frac{2}{2n+1}$。番号を付け替えて γ_2 とおく。$v_A(\beta_1 - \gamma_2) \gneq \frac{2}{2n+1}$ ということは $v_A(\gamma_2) = \frac{2}{2n+1}$ で、β_1, γ_2 を巾級数展開したとき $\frac{2}{2n+1}$ 次の項の係数が一致している。ところが Lemma より $i \neq 1$ なる β_i の展開の $\frac{2}{2n+1}$ 次の項とは係数が一致しない。よって $i \neq 1$ ならば $v_A(\beta_i - \gamma_2) = \frac{2}{2n+1}$。以下同様の操作を続けると最終的に $v_A(\beta_{n-1} - \gamma_n) \gneq \frac{2}{2n+1}$, $v_A(\beta_n - \gamma_n) = \frac{2}{2n+1}$ が得られ

$$v_A(\beta_n - \gamma_1) = \frac{2}{2n+1}$$

となる。これは左辺が真に小さいとした仮定に反する。従って $v_A(\gamma_j) \geq \frac{2}{2n+1}$。よって $\gamma_j \in \mathfrak{M}_A$。他の α'_i も $\mathfrak{M}_A$ の元となることがわかる。従って、

$$v_A(\alpha'_i) + 2v_A(\alpha'_i - \gamma_1) + \cdots + 2v_A(\alpha'_i - \gamma_n) = 2.$$

$v_A(\alpha'_i) \lneq \frac{2}{2n+1}$ と仮定すると $(2n+1)v_A(\alpha'_i) = 2$ となるがこれは矛盾。よって $\forall \alpha'_i$ について $v_A(\alpha'_i) = \frac{2}{2n+1}$, $v_A(\alpha'_i - \gamma_j) = \frac{2}{2n+1}$ となることがわかる。

最後に α'_i が重根になっていないことを示す。α'_i が重根とする. α'_i を

$$\begin{aligned} & (x(x-\gamma_1)^2 \cdots (x-\gamma_n)^2 + 4f(x))' \\ = \quad & (x-\gamma_1)^2 \cdots (x-\gamma_n)^2 + \cdots + 2x(x-\gamma_1)^2 \cdots (x-\gamma_n) + 4f'(x) \end{aligned}$$

に代入すると 0。また $\deg f \geq 1$ （$\because x = 0, \gamma_1, \ldots, \gamma_n$ は根ではない）。v_A を作用させると $\frac{4n}{2n+1} = 2 + (j-1)\frac{2}{2n+1} + v_A(j)$ となるがこのような正整数は存在しない。

参考文献

[1] W.Waterhouse and B.Weisfeiler, *One-dimensional affine group scemes*, J. of Alg.,Vol. 66, 1980, pp.550

[2] F.Oort,T.Sekiguchi and N.Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. scient. Éc. Norm. Sup., 4e série, t.22, 1989, pp.345

[3] R.Hartshorne, *Algebraic geometry*, Springer-Verlag, GTM 52

[4] J.P.Serre, *Algebraic groups and class fields*, Springer-Verlag, GTM 117

[5] 彌永昌吉　編, 数論, 岩波書店