数理解析研究所講究録
第 183 巻 1973 年 65-75

Affine line の k-form について.

Northern Illinois Univ. } 上林達治
京大 数研
阪大 理 宮西正宜

§1. 序

Affine line $\mathbb{A}^1$ は代数幾何学で扱われる variety のうち，最も簡単なものであるが，体の descent でどのように振舞うか，よく判っていない．特に純非分離拡大について判っていない．

本講演では，この問題について幾つかの注意と考察を与えることを目的とする．我々の問題は次のように述べられる：

k を標数 $p>0$ の任意の体，K を k 上の一変数代数函数体とする．K は singular place を持たないかも知れないが，持てば唯一つであると仮定し，更に k の代数的閉包 $\bar{k}$ との合成体 $K(\bar{k})$ が $\bar{k}$-rational になると仮定する．このとき，K の標準形を与えよ．

C を K の k-normal complete model，singular place があれば，それを P_∞ で表わす．singular place がないときは，P_∞ で k の純非分離拡大体上 rational な点を表わす．このとき

$C - P_\infty$ は affine line A^1 の k-form である．k' で k における k の完全閉包を表わせば，$C \otimes_k k' - P_\infty \cong A^1_{k'}$ (cf. Additive & Multiplicative Theorem 90 of Hilbert). 従って，我々の問題は次のようにもいい表わせる：

X を k 上定義された smooth affine curve で，$X_{k'} \cong A^1_{k'}$ となるものとすれば，X はどのような標準型に分類されるか？

§2. 環論的考察.

次の定理を証明する．

<u>Theorem</u>. k を標数 $p>0$ の体，k' を k の純非分離代数拡大体，A を有限生成 k-algebra，$A' = k' \otimes_k A$ として，次の条件を仮定しよう： k' は exponent 1 の拡大体, i.e., $k'^p \subseteq k$ で，A' は k' 上一変数多項式環に同型．このとき，A が k 上一変数多項式環に同型になる必要十分条件は A が素元分解環で，Spec(A) が k-rational point を持つことである．

<u>証明の概要</u>. (1) $[k' : k] = p^n$ とすれば，k' が k の exponent 1 の拡大体だから，k' の元 $\lambda_1, \cdots, \lambda_n$ が存在して，$\lambda_1, \cdots, \lambda_n \notin k$，$k' = k(\lambda_1) \otimes_k \cdots \otimes_k k(\lambda_n)$. 従って k' の中に k-derivations $d_1, \cdots, d_n$ が存在して； $d_i \neq 0$, $d_i^p = 0$, $d_i d_j = d_j d_i$, $d_i(\lambda_j) = \delta_{ij}$ (Kronecker's delta), $\forall\, i, j = 1, \cdots, n$.

d_i を A' の中の A-derivations $D_1, \cdots, D_n$ に，$D_i = d_i \otimes \mathrm{id}.$ と

おいて拡張する．やはり関係式：$D_i \neq 0$, $D_i^p = 0$, $D_i D_j = D_j D_i$, $D_i(x_j) = \delta_{ij}$ $(\forall i, j = 1, \cdots, n)$, $A = \{ a' \in A' \mid D_i(a') = 0, \forall i \}$ が成立する．

(2) まわりくどいが次の準備が必要である．A'を標数 $p > 0$ の Krull domain, K'をA'の商体，$(D_1, \ldots, D_n)$をK'の中の derivations の組で次の条件を充たすものとする：$D_i \neq 0$, $D_i^p = 0$, $D_i(A') \subseteq A'$, $D_i D_j = D_j D_i$, $\forall i, j = 1, \cdots, n$. $K = \{ x' \in K' \mid D_i(x') = 0, \forall i \}$, $A = K \cap A'$ とおけば，Aは Krull domain で $A'^p \subseteq A$. 従って，A'の $ht = 1$ の任意の素 ideal $\mathfrak{p}'$ のA上の分岐指数 $e_{\mathfrak{p}'}$ は 1 か又は p である．$C(A)$ 及び $C(A')$ で，それぞれA及びA'の divisor class groups を表わせば，群の準同型 $j : C(A) \longrightarrow C(A')$ が，$\sum n_{\mathfrak{p}} \mathfrak{p} \longmapsto \sum n_{\mathfrak{p}} e_{\mathfrak{p}'} \mathfrak{p}'$ ($\mathfrak{p}'$は$\mathfrak{p}$の上にあるA'の素 ideal) とおいて定義できる．Lで次のような形の logarithmic derivatives の組のなすアーベル群を表わそう：$\left(D_1(z)/z, \cdots, D_n(z)/z \right)$, $z \in K'^* = K' - (0)$, s.t. $D_i(z)/z \in A'$, $\forall i$. Lの加法は座標毎に行なわれる．$L_0 = \{ (D_1(u')/u', \cdots, D_n(u')/u') \mid u' \in A'^* = A'$の可逆元全体$\}$ とすれば，L_0はLの部分群．このとき，次の結果は容易に証明できる，(cf. [7])．

<u>Lemma</u>. 上記の記号と条件を仮定して，更にA'^*の元，$u'_1, \cdots, u'_n$ が存在して，$D_i(u'_j) = \delta_{ij}$, $\forall i, j = 1, \cdots, n$ を充

たすと仮定すれば，次の abel 群の完全列が存在する：

$$0 \longrightarrow L/L_0 \xrightarrow{\ i\ } C(A) \xrightarrow{\ j\ } C(A').$$

但し $i : L/L_0 \longrightarrow C(A)$ は $(D_1(z)/z, \dots, D_n(z)/z) \longmapsto \sum_{\mathfrak{p}'} (v_{\mathfrak{p}'}(z)/e_{\mathfrak{p}'})(\mathfrak{p}' \cap A)$ （$v_{\mathfrak{p}'}$ は $\mathfrak{p}'$ で定まる K' の normalized valuation）で定義される．又，j が surjective になる必要十分条件は，A' の任意の $ht=1$ prime ideal $\mathfrak{p}'$ について，$e_{\mathfrak{p}'}=1$ となることである．

(3) A が k 上一変数多項式環に同型ならば，A が素元分解環で，Spec(A) が k-rational point を持つことは明らかであるから，逆を証明しよう．上記(2)の Lemma を (1) の状況に応用しよう．仮定より $C(A)=(0)$ であるから，$L=L_0$．一方 A には極大 ideal $\mathfrak{m}$ が存在して，$A/\mathfrak{m}=k$．A' は A 上整だから，A' の極大 ideal $\mathfrak{m}'$ が存在して，$\mathfrak{m}=\mathfrak{m}' \cap A$，$A'/\mathfrak{m}'=k'$．　さて，$A'=k'[t]$ とすれば，A' は rank p^n の自由 A-加群でもあり，rank p^{n+1} の自由 $k[t^p]$-加群でもある．故に $A \neq k[t^p]$．$A-k[t^p]$ の元 f を t に関する次数（A' の中で考えて）が最小になるようにとる．$f=\alpha_0'+\alpha_1't+\cdots+\alpha_r't^r$，$\alpha_i' \in k'$ と書ける．必要ならば t を $t-(t \bmod \mathfrak{m}')$ で置きかえて，$t \equiv 0 \pmod{\mathfrak{m}'}$ と仮定してもよい．このとき，$f \equiv \alpha_0' \pmod{\mathfrak{m}'} \in k$．従って f を $f-\alpha_0'$ で置き換えて，$f \equiv 0 \pmod{\mathfrak{m}}$ としてよい．故に $f=t^s g$，$g=\alpha_s'+\cdots+\alpha_r't^{r-s}$，$\alpha_s' \neq 0$，$s \geq 1$

D_i を f に作用させて, $0 = D_i(f) = t^s D_i(g) + s t^{s-1} g D_i(t)$. よって, $t D_i(g) = -s g D_i(t)$. もし $p \mid s$ ならば, $D_i(g) = 0$ $\forall i$. 故に $g \in A$. $\deg_t g < \deg_t f$ だから, $g \in k[t^p]$. $\therefore$ $f = (t^{s/p})^p g \in k[t^p]$. これは矛盾であるから, $p \nmid s$. 故に $t \mid D_i(t)$, i.e. $(D_1(t)/t, \cdots, D_n(t)/t) \in L$. $L = L_0$ だから, $\exists \beta \in A'^* = k'^*$, s.t. $D_i(t/\beta) = 0$, $\forall i$. $u = t/\beta$ とおけば, $A' = k'[u]$ で, 容易に $A = k[u]$ がわかる. 証終.

定理の2つの条件のうち, どの一つを省略しても定理は成立しないことを注意しておこう.

§3. 幾何学的考察.

X が affine line A^1 の k-form のとき, X の k-normal completion を C, $P_\infty = C - X$ とおく。P_∞ は one-place point で, singular point があれば P_∞ である.

<u>Lemma 1</u>. P_∞ は k の純非分離代数拡大体上 rational である。

C は k 上 proper だから, その Picard scheme $\underline{\mathrm{Pic}}_{C/k}$ は存在し, 単位元を含む連結成分 $\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は k 上有限生成な group scheme である. $\underline{\mathrm{Pic}}$ の性質のうち, 我々の使う性質は次の通りである.

<u>Lemma 2</u>. k 上 proper scheme X が条件: $H^0(X, \mathcal{O}_X) = k$,

$X \ni k$-rational point，を充たすならば，次の事柄が成立する。

(1) $\forall S \in (Sch/k)$ について，$\mathrm{Pic}(X_S) \cong \underline{\mathrm{Pic}}_{X/k}(S) \times \mathrm{Pic}(S)$.
但し $\mathrm{Pic}(X_S) = H^1(X_S, \mathcal{O}^*_{X_S})$ etc.

(1)′ k の任意の拡大体 k' に対して，$\mathrm{Pic}(X_{k'}) = \underline{\mathrm{Pic}}_{X/k}(k')$.

(2) k の任意の拡大体 k' について，$\underline{\mathrm{Pic}}_{X_{k'}/k'} \cong \underline{\mathrm{Pic}}_{X/k} \otimes_k k'$.

Lemma 1 の前の記号法に房って，次の二つの結果を得る．

<u>Lemma 3</u>. $\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は smooth affine k-group scheme である．更に $X = C - P_\infty$ が k-rational point P_0 をもてば，k-schemes の morphism $i : C - \{P_\infty\} \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{C/k}$ が存在して，k の任意の拡大体 k' と $\forall Q \in C(k') - P_\infty$ について，$i(Q) = Q - P_0$.

<u>Lemma 4</u>. C を smooth complete k-curve として，次の条件を仮定する：k の純非分離代数拡大体 k' が存在して，$C \otimes_k k'$ は k'-rational．標数 $p = 2$ ならば，C は k-rational point をもつと仮定する．このとき C は k-rational である．

$p = 2$ の場合，C に k-rational point が存在することを仮定しなければ，Lemma 4 は成立しない。<u>反例</u>. $k = F_2(t, u)$, t, u は変数. C を方程式 $Y^2 = tZ^2 + XZ + uX^2$ で定義される plane curve とすれば，C は k-rational ではない。

Lemmas 1 〜 4 を併せれば，次の結果を得る．

<u>Theorem 5</u>. X, C, P_0, P_∞ を Lemma 3 のように取れば，次の条件は互いに同値である：

(1) $i : C - \{P_\infty\} \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{C/k}$ は closed immersion で $\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は group scheme として，i の image によって生成される．

(2) $\dim \underline{\mathrm{Pic}}^{\circ}_{C/k} > 0$, i.e., C の arithmetic genus > 0.

(3) C は k-rational ではない．

(4) $C - \{P_\infty\}$ は smooth complete k-curve に embed することができない．

実際，$\underline{\mathrm{Pic}}^{\circ}_{C/k} \otimes_k \bar{k}$ は $C \otimes_k \bar{k}$ の generalized Jacobian variety になる．（$\bar{k}$ は k の代数的閉包）．generalized Jacobian variety のもつ性質より次の結果を得る．

<u>Theorem 6</u>. $\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は unipotent k-group である．より精密には，$\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は有限次元 Witt vector groups の直積の k-form である． $\underline{\mathrm{Pic}}^{\circ}_{C/k} \neq 0$ ならば，$\underline{\mathrm{Pic}}^{\circ}_{C/k}$ は k-wound group (i.e., k-morphism $\mathbb{A}^1 \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{C/k}$ が存在すれば，それは constant morphism) である．

Theorem 6 の後半を証明するのには，次の結果を使う．

<u>Lemma 7</u>. V を k-regular proper integral scheme, U を smooth k-scheme として，次の条件が充たされると仮定

しよう： V は k-rational point をもつか，k 上 generically separable である．そのとき，任意の rational map $f: V \longrightarrow \underline{\mathrm{Pic}}_{V/k}$ は V のすべての点で正則である．

$\mathbb{A}^1$ の k-forms を完全に分類することは，今のところできていないが，arithmetic genus が 0 又は 1 ならば可能である．

<u>Genus 0 の場合</u>．a を $k-k^p$ の元，n を自然数として，(a, n) に対して，$\mathbb{P}^1$ の embedding $\varphi: \mathbb{P}^1 \longrightarrow \mathbb{P}^{p^n}$ を $t \longmapsto (1, t, \cdots, t^{p^n-1}, t^{p^n}-a)$ で与える．但し t は $\mathbb{P}^1$ の non-homogeneous 座標である．$\mathbb{P}^1$ の $t^{p^n}=a$ で定まる点を P_∞ として，$X_{a,n} = \varphi(\mathbb{P}^1 - \{P_\infty\})$ とおく．

<u>Theorem 8</u>. (1) $\mathbb{A}^1$ の k-rational k-form は $\mathbb{A}^1$ 又は $X_{a,n}$ に k-同型である．

(2) $X_{a,n}$ は $\mathbb{A}^1$ に同型でない，$\mathbb{A}^1$ の k-rational k-form である．

(3) $X_{a,n} \cong X_{b,m} \iff$ (i) $m = n$

(ii) $\exists \alpha, \beta, \gamma, \delta \in k^{p^n}$ s.t. $\alpha\delta - \beta\gamma \neq 0$, $\dfrac{\alpha a+\beta}{\gamma a+\delta} = b$.

標数 $p \geqq 3$ ならば，arithmetic genus が 0 である $\mathbb{A}^1$ の k-form は必ず k-rational である．

Genus 1 の場合. 次の定理にまとめられる.

Theorem 9. $\mathbb{A}^1$ の k-form が k-rational point をもち, arithmetic genus が 1 ならば, 次の Russel 型 k-groups のどれかに同型である:

(1) $p = 3$, $y^3 = x - \gamma x^3$, $\gamma \in k - k^3$

(2) $p = 2$, $y^4 = x + \beta x^2 + \gamma^2 x^4$, β 又は $\gamma \in k - k^2$ $(\beta, \gamma \in k)$.

arithmetic genus が 1 の $\mathbb{A}^1$ の k-form が k-rational point を持たなければ, それは上記の Russel 型 k-group の principal homogeneous space である, (cf. [2]).

Remark. $G_a \times G_a$ の中で, 方程式

$$y^{p^n} = x + a_1 x^p + \cdots + a_r x^{p^r}, \quad a_1, \ldots, a_r \in k$$

$$a_1, \ldots, a_r \text{ のどれかは } \notin k^p$$

で与えられる, dim = 1 の k-group を Russel 型 k-group という, (cf. [2]). Russel 型 k-group は $\mathbb{A}^1$ の k-form である. $\mathbb{A}^1$ の k-form がいつ Russel 型 k-group になるかという問に対する答えは次の定理で与えられる.

Theorem 10. X, C, P_0, P_∞ を Lemma 3 と同じように取れば, 次の条件は同値である:

(1) X は P_0 を単位元にするような k-group scheme の構造をもつ.

(2) X は Russel 型 k-group に k-同型である.

(3) k_s を k の分離代数閉包とすると, $\#(\underline{\mathrm{Aut}}_{C/k}(k_s)) = \infty$

もし X の arithmetic genus $\neq 0$ ならば, 上の条件は次の条件に同値である;

(4) 1次元 unipotent k-group H と surjective homom.
$\rho : \underline{\mathrm{Pic}}^{\circ}_{C/k} \longrightarrow H$ が存在して, $\rho \cdot i = X$ から H への k-同型, $\rho \cdot i(P_0) = H$ の単位元.

<u>Conjecture</u>. $\mathbb{A}^1$ の k-form X は, X の arithmetic genus $\geqq 2$ ならば, ある Russel 型 k-group の principal homogeneous space である.

定理7を考慮すれば, 次の結果を得る.

<u>Theorem 11</u>. G が Russel 型 k-group, $K = k(G)$ が k 上の G の函数体ならば, K が k-rational になる必要十分条件は, $p = 2$ で G の定義方程式: $y^2 = x + ax^2$, $a \in k - k^2$ となることである.

<u>Theorem 12</u>. G を Russel 型 k-group, C を G の k-normal completion, $P_\infty = C - G$ とおけば, 次の二つの完全列を得る:

(1) $0 \longrightarrow \mathbb{Z} \longrightarrow \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}(G) \longrightarrow 0$

(2) $0 \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{C/k}(k) \longrightarrow \mathrm{Pic}(G) \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$.

ここで p^n は, $\bar{k}$ を k の代数閉包とするとき, $\bar{k}(G)$ の P_∞ 上の唯一つの place が $k(G)$ 上持つ分岐指数である. もし G が

定義式 $y^{p^r} = x + a_1 x^p + \cdots + a_m x^{p^m}$ で与えられるならば、$p^r \leq p^n$.

文献

[1] P. Samuel; On unique factorization domains, Tata Inst. Fund. Res., Bombay, 1964.

[2] P. Russell; Forms of the affine line and its additive group, Pacif. J. Math., 32 (1970), 527–539.