種数1の正標数代数曲線の同型類の
幾何的基本群による復元

更科 明 (京都大学)

1 Grothendieck 予想

k を体, G_k を k の絶対ガロア群, U を代数多様体 (k 上の有限型, 分離的, 幾何的に連結なスキーム), $\pi_1(U)$ を U のエタール基本群とする. A. Grothendieck により, k が数体などの体のとき Grothendieck 予想と呼ばれる次のような哲学が提唱された.

U が "遠アーベル多様体" のとき, U の幾何は $\pi_1(U) \twoheadrightarrow G_k$ により決定される.

この予想に関して以下のような結果が良く知られている.

定理 1 ([3]). k が劣 p 数体 (i.e. Q_p の有限生成拡大体の部分体), U_1, U_2 が k 上の双曲的曲線 (i.e. $2g+n-2>0$, ここで g は種数, n はカスプの数) のとき

$$\begin{tikzcd} U_1 \arrow[rr, dash, "\sim"] \arrow[dr] & & U_2 \arrow[dl] \\ & Spec(k) & \end{tikzcd} \quad \Longleftrightarrow \quad \begin{tikzcd} \pi_1(U_1) \arrow[rr, dash, "\sim"] \arrow[dr] & & \pi_1(U_2) \arrow[dl] \\ & G_k & \end{tikzcd}$$

上の定理は数理研の望月新一氏によって示された劣 p 数体上の双曲的曲線に対する Grothendieck 予想の系である.

k が標数 0 の代数閉体, U が曲線 (i.e. k 上の非特異な有限型整分離的 1 次元スキーム) のとき $\pi_1(U)$ の位相群としての同型類は U のカスプの数と種数によって定まるので U のスキームとしての同型類を $\pi_1(U)$ から復元することはできない ([1, Exposé 12]).

しかし k が正標数の場合はカスプの数と種数のような簡単な不変量から $\pi_1(U)$ の同型類を決定することはできない. また多くのスキーム論的普遍量がエタール基本群から復元されることが知られており, その一つとして以下の結果が知られている.

定理 2 ([2, Theorem 3.5]). p : 素数, $k \simeq \overline{\mathbb{F}}_p$, U_1, U_2 が k 上の曲線, $g(U_1)=0$ のとき

$$U_1 \simeq U_2 \text{ (スキームとして)} \iff \pi_1(U_1) \simeq \pi_1(U_2).$$

種数が 1 以上の場合にも同様の結果が成り立つか研究し以下の結果を得た.

定理 3 (S). p : 奇素数, $k \simeq \overline{\mathbb{F}}_p$, U_1, U_2 が k 上の曲線, $(g(U_1), n(U_1)) = (1,1)$ のとき

$$U_1 \simeq U_2 \text{ (スキームとして)} \iff \pi_1(U_1) \simeq \pi_1(U_2).$$

2　定理 3 の証明のアイデア

補題 4 ([2])**.**

$$\pi_1(U_1) \simeq \pi_1(U_2) \Rightarrow (g(U_1), n(U_1)) = (g(U_2), n(U_2)).$$

補題 4 より $(g(U_2), n(U_2)) = (1, 1)$ を仮定して良い．E_1 (*resp.* E_2) を U_1 (*resp.* U_2) のコンパクト化, $E_1 \backslash U_1 = \{\mathcal{O}_1\}, E_2 \backslash U_2 = \{\mathcal{O}_2\}$ とおく．

補題 5. 任意の $m \in 2\mathbb{Z}_{>0}$ に対し $[m] : E \to E$ の制限 $E \backslash E[m] \to E \backslash \mathcal{O}$ から定まる開部分群 $\pi_1(E \backslash E[m]) \hookrightarrow \pi_1(E \backslash \mathcal{O})$ は $\pi_1(E \backslash \mathcal{O})$ から群論的に復元できる．

補題 6 ([2])**.** 自然な写像 $Iso(\pi_1(U_1), \pi_1(U_2)) \to Bij(S_{U_1}, S_{U_2})$ が存在する．

補題 5, 補題 6 より $E_1, E_2, m \in 2\mathbb{Z}_{>0}$ に対し自然な全単射 $\phi : E_1[m] \simeq E_2[m]$ が定まる．$\mathbb{P}^2$ への埋め込みをうまくとり，E_1 は $y^2 = x(x-1)(x-\lambda_1)$ で定義され, $\mathcal{O}_1 = \infty$, E_2 は $y^2 = x(x-1)(x-\lambda_2)$ で定義され, $\mathcal{O}_2 = \infty$, $\phi((\lambda, 0)) = (\lambda_2, 0)$, $\phi((i, 0)) = (i, 0)$ $(i = 0, 1)$ が成り立つとして良い．

$\mathbb{P}^1$ の 2 点 P_0, P_∞ を定めれば全単射 $k \simeq \mathbb{P}^1 \backslash \{P_\infty\}$ $(0 \leftrightarrow P_0)$ から誘導される加法が $\mathbb{P}^1 \backslash \{P_\infty\}$ に定まる．E_1, E_2 に対して ∞ を分岐点とする $\mathbb{P}^1$ への射影 $(x_i : E_i \to \mathbb{P}^1)$ を考え, $(0, 0)$ の像を P_0, ∞ の像を P_∞ とする加法に関する $x_i(E_i[m] \backslash \{\mathcal{O}_i\})$ の線形関係を考える．

補題 7. 楕円曲線 E, ∞ を分岐点とする射影 $x : E \to \mathbb{P}^1$, 4 以上の偶数 m, 及び $a_P \in \mathbb{F}_p$ $(P \in x(E[m]) \backslash \{P_0 = x(\lambda_0), P_\infty = x(\lambda_\infty)\}$ が与えられたとき

$$\sum_{P \in x(E[m]) \backslash \{P_0, P_\infty\}} a_P P = P_0 \quad (P_0, P_\infty \text{に関する } \mathbb{P}^1(k) \backslash \{P_\infty\} \text{ 上の加法})$$

が成り立つか否かは $\pi_1(E \backslash \mathcal{O})$ から群論的に復元できる．

また ϕ は楕円曲線の群構造に関して同型．よって標語的に言えば「ϕ は楕円曲線の加法と $\mathbb{P}^1$ の加法を共に保っている」ということになる．この二つの加法を組み合わせることで λ_1 と λ_2 の $\mathbb{F}_p$ 上の最小多項式が等しいことが示される．λ_1 を λ_2 へ移す k の同型で基底変換することで U_1 と U_2 の同型を得る．

参考文献

[1] A. Grothendieck, Revêtemental étales et groupe fondamental, SGA 1, Lecture Notes in Mathematics, 224, Springer-Verlag, Berlin-New York, 1971.

[2] A. Tamagawa, On the fundamental groups of curves over algebraically closed fields of characteristic > 0, Internat. Math. Res. Notices 1999, no. 16, 853–873.

[3] S. Mochizuki, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, J. Math. Sci. Univ. Tokyo **3** (1996), no. 3, 571–627.