数理解析研究所講究録 1283 巻 2002 年 7-20

Hrushovski's New Proof of Manin-Mumford Conjecture

板井　昌典 (ITAI Masanori)
東海大学　理学部　情報数理学科
(Department of Mathematical Sciences, Tokai University)

1　はじめに

幾何的モデル理論の数論幾何への応用として，E. Hrushovski による幾何的 Mordell-Lang 予想の解決は有名である．ザリスキー幾何の理論を用いて，すべての標数に対して統一的論法で予想を解いたのであった．標数 0 の場合はすでに A. Buium によって微分代数的手法で解かれていたが，すべての正標数に対する解決は Hrushovski による画期的な結果である．

ここでは，やはり Hrushovski による数論幾何への応用として，Manin-Mumford 予想に対する，新たな視点からの別証明について解説する．

2　Manin-Mumford 予想

可換群 G と $0 \neq g \in G$ に対して，$ng = \underbrace{g + \cdots + g}_{n\text{回}} = 0$ となる自然数 n が存在する時，g を G の n-torsion 点という．G の n-torsion 点全体の集合を $\mathrm{Tor}_n(G)$ と書き，$\mathrm{Tor}(G) = \bigcup_n \mathrm{Tor}_n(G) \cup \{0\}$ とおく．$\mathrm{Tor}(G)$ は G の部分群になる．

Manin-Mumford 予想というのは $\mathrm{Tor}(G)$ の構造に関する次のような予想である．

Manin-Mumford 予想
C ：種数 2 以上の代数曲線，$J(C)$ ：C のヤコビ多様体，$C \subset J(C)$ と考える．
C 上には $J(C)$ の torsion points は有限個しかない．

・ちなみに，種数 1 の場合，C は楕円曲線である．この場合 $J(C) = C$ であり，torsion points は無限個ある．群 G に対して $\mathrm{Tor}(G)$ の構造が分かれば，有限性は自然な帰結として得られる．アーベル多様体に関しては次の結果が有名である．

Theorem 1 (Raynaud, 1983)
A をアーベル多様体，X を部分多様体とする．ともにある数体 K 上定義されている．Tor(A) を $A(K^a)$ の torsion pts 全体の群とすると，

$$\mathrm{Tor}(A) \cap X = \bigcup_{i=1}^{n} (\mathrm{Tor}(A_i) + c_i)$$

である．ただし，A_i は A の部分群多様体，$c_i \in A$，K^a は K の代数的閉包とする．

アーベル多様体は完備な代数群である．代数群の完備性を仮定せず，単に可換性のみを仮定しても同様の結果が得られることを，Hrushovski が示した．

Theorem 2 (Hrushovski)
G を可換代数群，X を部分多様体とする．ともにある数体 K 上定義されているとすると

$$\mathrm{Tor}(G) \cap X = \bigcup_{i=1}^{n} (\mathrm{Tor}(G_i) + c_i)$$

である．ただし，G_i は G の部分代数群，$c_i \in G$ である．さらに，n の大きさを effective に押さえることが出来る．すなわち，

$$n \leq c \deg(X)^e$$

であるような定数 c, e が存在する．ここで c, e は G と G の２つの good reductions p, q だけに依存して決まる．

3 1-基底群 (One-based Groups)

幾何的モデル理論を用いて解く場合，1-基底群と呼ばれる群の構造定理が活躍する．次に述べる基本性質のうち，3 番目が特に重要である．

Fact 1 *G を 1-基底群とする．*

1. 加群は 1-基底群である．よって可換群は 1-基底群である．
2. 連結な 1-基底群は可換群である．(一般には，可換群 × 有限)
3. G の任意の定義可能部分集合 X は，有限個の定義可能部分群たちの剰余類のブール和である．

1-基底群の典型例である加群のモデル理論について考えてみよう．R を乗法の単位元 1 を持つ，可換環とし，R-加群の言語，$L_R = \{+, 0, \{f_r : r \in R\}\}$，（ただし f_r は r 倍を表す 1 変数関数記号）を一つ固定する．

Example 1
$\mathbf{Z}$-加群としての，$(\mathbf{Z}, +, 0, \{f_n : n \in \mathbf{Z}\})$ の定義可能部分集合 X の形を考える．$x \equiv k \mod n$ という関係は，論理式 $\exists y\ (x = f_n(y) + k)$ で定義される．したがって定義可能集合 X は $x \equiv k \mod n$ の形をした論理式のブール和によって定義されていることが分かる．これはまさに Raynaud の定理や Hrushovski の定理における $\mathrm{Tor}(G)$ の構造と同じである．

一般の R-加群に関しては，次のような構造定理が得られている．

Theorem 3
M を R-加群とする．$\psi(\bar{x})$ を論理式とする．p.p-論理式のブール和になっている論理式 $\psi^*(\bar{x})$ が存在して，

$$M \models \psi(\bar{x}) \longleftrightarrow \psi^*(\bar{x})$$

*が成り立つ．*ここで，p.p-論理式というのは，上の $x \equiv k \mod n$ と同様のことを加群の言語 L_R で表現した論理式のことである．

したがって本題に戻れば，アーベル多様体 A あるいは可換代数群 A に対して，$\mathrm{Tor}(A)$ が 1-基底群であれば一件落着である．しかし大きな問題が待ち構えている．点 x が torsion point であるということの定義を振り返ってみよう．

$$\mathrm{Tor}(A) \ni x \iff \exists n \in \mathbf{N}\ (nx = 0)$$

である．ここで,「$\exists n \in \mathbf{N}$」の部分が問題なのである．幾何的モデル理論ではこのような量記号は扱えないのである．つまり，$\mathrm{Tor}(A)$ という群をモデル理論で直接扱う事が出来ない．

ではどうすればよいのか？
$\mathrm{Tor}(A)$ の代わりに，$\mathrm{Tor}(A)$ を含む 1-基底群を探せばよい．そのような群を探すために difference fields のモデル理論が登場するのである．すなわち，体 K とその自己同型 σ を一緒に考えるモデル理論である．特に ACFA と呼ばれる，代数的閉体と自己同型 σ を一緒に考えるモデル理論が活躍するのである．ACFA に関しては，本講究録にある桔梗宏孝氏の解説を参照されたい．

4 幾何的Mordell-Lang予想との関連

ここで幾何的Mordell-Lang予想との関連を考えてみよう．Hrushovskiが証明したのは次の結果である．

Theorem 4

$k_0 \subset K$ を異なる代数的閉体とする．K 上で定義されたアーベル多様体 A と，A の無限部分多様体 X を考える．

Γ を $A(K)$ のランク有限な部分群とする．さらに，$\mathrm{Stab}_X = \{a \in A : a + X = X\}$ は有限であるとする．

このとき次の1または2のいずれかが成り立つ．

1. $X \cap \Gamma$ は X でザリスキー稠密でないか，または
2. A の部分アーベル多様体 B，k_0 上定義されたアーベル多様体 S，そして k_0 上定義されている S の部分多様体 X_0 と K 上の同型射 $h : B \longrightarrow S \otimes_{k_0} K$ が存在して

$$X = a_0 + h^{-1}(X_0 \otimes_{k_0} K) \ (a_0 \in A)$$

となっている．

実は上の定理を幾何的モデル理論を用いて証明する場合，**ランク有限な群** Γ を扱うことが出来ないのである．ランク有限の定義にはやはり「$\exists n \in \mathbf{N}$」が必要だからである．この定理を証明するということは，場合1または場合2のいずれかが成り立つということを示すことである．

1. この場合については，Γ を含む1-基底群を探さなければならない．
   - 標数0の場合：differentially closed fields のモデル理論を用いる
   - 正標数の場合：separably closed fields のモデル理論を用いる
2. この場合ザリスキー幾何の理論を用いて，k_0 と同型な体を再構成する．

このように幾何的Mordell-Lang予想の解決にはザリスキー幾何の理論が必要[1]であるが，Manin-Mumford予想では，ザリスキー幾何の理論は不要である．

---

[1]標数0の場合，ザリスキー幾何は不要であることが2002年初頭に証明された．正標数の場合は依然として必要である．

5 Prime-to-p Torsions

$\mathrm{Tor}(A)$ を含むような 1-基底群を探さなければならないが，その前により簡単な $\mathrm{Tor}'_p(A)$ について考えることにする．

p を素数，$q = p^n$ $(n \in \omega)$ とし $k = \mathrm{GF}(q)$ を標数 p の有限体とする．また k^a を k の代数的閉包とする．

- $\mathrm{Tor}'_p(A) = \{a \in A : \exists n\ (na = 0)$ ただし，n は p と互いに素$\}$
- $\phi_q : x \longmapsto x^q : k^a$ の Frobenius 自己同型

とおく．参考文献にあげた Hrushovski の論文にある次の補題が重要な働きをする．

Lemma 5.0.9 (Hrushovski の論文の p. 104)
A を k 上の可換代数群とする．このとき

$$F(\phi_q)(a) = 0\ (\forall a \in \mathrm{Tor}'_p(A))$$

を満たす $F(T) \in \mathbf{Z}[T]$ が存在する．ただし，$F(T)$ は1のべき乗根を根として持たない．また，多項式 $F[T]$ は次の性質を持つ．

- $\deg(F) \leq 2\dim(A)$
- F の係数の絶対値の和 $\leq (1 + q^{1/2})^{2\dim(A)}$

この補題があるので，$\mathrm{Tor}'_p(A)$ で 0 となるような自己同型を規定する整数係数多項式の存在が保障される．そじてこのような多項式が存在するので，difference fields のモデル理論が活躍出来る．ACFA の結果を駆使して，$\mathrm{Tor}'_p(A)$ を含む 1-基底群を探すのである．その結果として Manin-Mumford 予想を解く事が出来る．[2]

Lemma 5.0.9 の証明
A を k 上の可換代数群とする．

Step 1: A の分解

$$0 \to L \to A \to \overline{A}\ \ (k \text{ 上の完全列})$$

を考える．ここで，L は線形代数群，$\overline{A}$ はアーベル多様体である．よって

$$0 \to \mathrm{Tor}(L) \to \mathrm{Tor}(A) \to \mathrm{Tor}(\overline{A})$$

[2]Hrushovski は 1-基底的 (one based) ではなく algebraically modular と呼ぶ．

である．したがって，

$$(\ F_1(\phi_q)|\mathrm{Tor}(L)=0 \wedge F_2(\phi_q)|\mathrm{Tor}(\overline{A})=0\ ) \implies F_1F_2(\phi_q)|\mathrm{Tor}(A)=0$$

である．ここで，$F_1(\phi_q)|\mathrm{Tor}(L)=0$ というのは，任意の $a \in \mathrm{Tor}(L)$ に対して $F_1(\phi_q)(a)=0$ が成り立つということである．

Step 2: 3 つの場合がある．
①：A がアーベル多様体のとき．Weil の古典的結果を用いて，多項式 $F[T]$ の存在を示す．得られる多項式 $F[T]$ は，次数 $2\dim(A)$ のモニックで，固有値はすべて $|q^{1/2}|$ である．

概略：
l を k の標数と異なる素数とする．

$$T^* = \{(a_1, a_2, \dots) : a_i \in A,\ l\cdot a_1 = 0,\ l\cdot a_{i+1} = a_i\}$$

とおくと，T^* は自由 $\mathbf{Z}_l$-加群であり，$\dim(T^*) = 2\dim(A)$ である．

任意の $\alpha \in \mathrm{End}(A)$ は $\mathbf{Z}_l$-linear map として T^* に作用する．一方，ratinal endmorphism α は，T^* への作用によって決まり，Frobenius ϕ_q は A の rational end を定める．また任意の $F(T) \in \mathbf{Z}[T]$ に対して，

$$F(\phi_q) \text{ is } 0 \text{ on } A \iff F(\phi_q) \text{ is } 0 \text{ on } T^*$$

である．$P(T)$ を ϕ_q の特性多項式，すなわち $\det(T-\phi_q)$ とする．$P(\phi_q)$ は T^* 上 0 である．ここで，$P(T) \in \mathbf{Z}[T]$ であることを示すのがポイントである (Weil の理論が必要)．

ϕ_q を $T^* \otimes \mathbf{Q}_l$ の $\mathbf{Q}_l$-線形変換とみたとき，$P(T)$ の根と ϕ_q の固有値が一致する．

もしある固有値が 1 のべき乗根ならば，1 は ϕ_q^N の固有値（N は自然数）よって，$\phi_q^N(v)=v$ となる $0 \neq v \in T^*$ が存在する．ϕ_q^N は A の無限個の元を固定する．ところで $\mathrm{Fix}(\phi_q^N)$ は有限だから矛盾する．したがって，A 上で $P(\phi_q)$ は 0 である．

参考文献

A. Weil, *Courbes algébriques et variété abélienne*

A. Pillay, **Fact 2.2**, p. 198

②：A が algebraic torus のとき．

$\mathrm{GF}(q^l)$ 上定義された同型写像 $g : A \longrightarrow \mathbf{G}_m^n$ が存在する．$\phi_q(g) : A \longrightarrow \mathbf{G}_m^n$ もやはり同型写像である．$\psi = g \circ \phi_q(g)^{-1}$ とおくと，ψ は $\mathbf{G}_m^n$ の自己同型であり，$\psi \in \mathrm{GL}_n(\mathbf{Z})$ である．

ψ は ϕ_q で動かない．また，$\psi^l = \psi \circ \phi_q(\psi) \circ \cdots \circ \psi_q^{l-1} = id$ なので g は ϕ_q^l で動かないことに注意する．

このgを用いると，$(A, \phi_q) \cong (G_m^n, g\phi_q g^{-1})$ であることが分かる．

$g\phi_q g^{-1} = \psi \circ \phi_q$ かつ $(\psi \circ \phi_q)^l = (\phi_q)^l = \phi_{q^l}$ なので，A が algebraic torus である場合は多項式として $F[T] = T^l - q^l$ を使えばよい．

③ : A が unipotent group のとき．

$\mathrm{Tor}_{p'}(A) = \emptyset$ なので $F[T] = 1$ とする．

標数 p から標数 0 へ

最終的には数体上で議論しなければならないので，Lemma 5.0.9 を標数 0 へ持ち上げなければならない．A を数体 K 上の，連結な可換代数群とし，$\wp$ を a prime of good reduction とする．

L を K_p の完備化の極大な非分岐拡大とすると，$\mathrm{Tor}_{p'}(A) \subseteq A(L)$ である．

さて，k^a の Frobenius 自己同型 ϕ_q は L の自己同型 ϕ へ持ち上げられる（理由 : algebraically closed valued fields の理論はＱＥを持つので）．また，L から k^a への制限は，$\mathrm{Tor}_{p'}(A)$ 上の 1 対 1 写像を定義する．

任意の多項式 $F[T] \in \mathbf{Z}[T]$ に対して，

$$F(\phi)(a) = 0\ (\forall a \in \mathrm{Tor}_{p'}(A)) \iff F(\phi_q)(a) = 0\ (\forall a \in \mathrm{Tor}_{p'}(A_k))$$

である．これらを用いて，Lemma 5.0.9 を次のように標数 0 版へと持ち上げる．

Lemma 5.0.10.

σ_0 を K^a の自己同型とする．このとき，1 のべき乗根を解としてもたない，次数 $\dim(A)$ の多項式 $F[T] \in \mathbf{Z}[T]$ で，F の係数の絶対値の和 $\leq (1 + q^{1/2})^{2\dim(A)}$ であるようなものが存在して，

$$F(\sigma_0)(a) = 0\ (\forall a \in \mathrm{Tor}_{p'}(A))$$

が成り立つ．

以後，$(K^a, \sigma_0) \subset (L, \sigma)$ を difference field とすると，

$$F(\sigma)(a) = 0,\ (\forall a \in \mathrm{Tor}_{p'}(A))$$

なので，(K^a, σ_0) を generic な difference fileds に埋め込む．

5.1. ACFA の登場

ACFA に関しては桔梗氏の解説を参照して欲しいが，1-基底群に関連した定理を 3 つ列挙しておく．

Proposition 1

$(K,\sigma) \models$ ACFA，$E = \mathrm{acl}_\sigma(E) \subseteq K$ とし，
p : E 上の非自明な modular タイプ，$\mathrm{SU}(p) = 1$ とすると

$$p \not\perp \begin{cases} \text{単純アーベル多様体，または} \\ \mathbf{G}_m \end{cases}$$

Theorem (Dichotomy)

p は $E = \mathrm{acl}_\sigma(E)$ 上の SU-rank 1 のタイプとすると

$p \not\perp (\sigma(x) = x)$ または (p は modular, stable, stably embedded, stationary)

さらに，

$$p \not\perp (\sigma(x) = x) \iff \begin{cases} \deg_\sigma(p) = 1，\text{かつ} \\ \text{自然数 } N \text{ が存在して，任意の } k \in \mathbf{Z} \text{ に対して} \\ [E(a, \sigma^k(a)) : E(a)] \leq N \end{cases}$$

Proposition 2

K を ACFA のモデルとする．H を K 上定義された代数群，G を $\mathrm{SU}(G) < \omega$ であるような $H(K)$ の定義可能部分群とする．さらに，G は $E = \mathrm{acl}_\sigma(E)$ 上定義されていて，$G \perp$ all fixed fields とする．

このとき，量記号を用いずに定義される任意の部分集合 $X \subseteq H(K)^m$ に対して，

$$X \cap G^m = \text{量記号なしで } E \text{ 上定義可能な } G^m \text{ の有限個の剰余類のブール和}$$

である．

5.2 ACFA の 1-基底群

Definition 1

A を可換代数群とし，V を極大な，vector subgroup (つまり $\cong (\mathbf{G}_a)^m$) とする．Y を $V(K)$ の定義可能部分集合，C を $A(K)$ の定義可能部分群の剰余類とする．このとき，$Y + C$ を *special* と呼ぶ．

Theorem 5

$(K,\sigma) \models$ ACFA とし，A を $\mathrm{Fix}(\sigma)$ 上定義された可換代数群とする．

1 のべき乗根を解に持たない $F[T] \in \mathbf{Z}[T]$ に対して，$G = \{g \in A(K) : F(\sigma)(g) = 0\}$ とおくと，

1. G のすべての定義可能部分集合は，G の special subsets の有限ブール和である．

2. X が A の部分多様体であるとき，$X \cap G$ は A の special 部分多様体の有限和である．

$\mathrm{Tor}_{p'}(A) \subseteq G$ となっているので，G がこの Porposition 1 のような性質を持てば，$\mathrm{Tor}'_p(A)$ も同様の性質を持ち，$\mathrm{Tor}'_p(A)$ に関する Manin-Mumford 予想を解くことが出来る．

6 All Torsions

もともとの問題は $\mathrm{Tor}'p(A)$ ではなくて $\mathrm{Tor}(A)$ に関するものである．$\mathrm{Tor}'_p(A)$ の結果を利用して $\mathrm{Tor}(A)$ に関する結論を得るには 3 つの方法がある．

1 つ目の道：2 つの自己同型を用いる

Proposition 6.1.1 (Hrushovski, p. 106)
A を数体 K 上定義された準アーベル多様体，X を A の部分多様体とすると，

$$X \cap \mathrm{Tor}(A) = \ A \text{ の有限個の群部分多様体の剰余類の和.}$$

となる．

概要：

$p \neq l$ を A の異なる good reduction とする．$\mathrm{Tor}(A) = \mathrm{Tor}_{p'}(A) \oplus \mathrm{Tor}_{l'}(A)$ と考える．

このとき，σ, τ，$F_p[T], F_l[T] \in \mathbf{Z}[T]$ が Lemma 5.0.9 より存在する．$F_p(\sigma)$ は $\mathrm{Tor}_{p'}(A)$ で 0 であり，$F_l(\tau)$ は $\mathrm{Tor}_{l'}(A)$ 上で 0 である．

$A_p = \mathrm{Ker}(F_p(\sigma))$，$A_l = \mathrm{Ker}(F_l(\tau))$ とおく．また $\mathcal{F}$ を σ, τ で生成される自由群とする．

このとき，$A_p^{\mathcal{F}} \times A_l^{\mathcal{F}}$ は one-based (algebraically modular) (Prop. 4.5.2) である．よって $A_p^{\mathcal{F}} + A_l^{\mathcal{F}}$ も one-based である．

$\mathrm{Tor}_{p'}(A) \subseteq A_p$ かつ $\mathrm{Tor}_{p'}$ は $\mathcal{F}$-不変なので $\mathrm{Tor}_{p'}(A) \subseteq A_p^{\mathcal{F}}$ である．同様に $\mathrm{Tor}_{l'}(A) \subseteq A_l^{\mathcal{F}}$ である．

よって $T \subset A^{\mathcal{F}}$ なので T は one based (alg. modular) である．

2 つ目の道：1 つの自己同型

A を数体 K 上定義された可換代数群，V を A の極大 vector subgroup とし，$B = A/V$ とおく．

目標 : $G(\sigma')|\mathrm{Tor}(A) = 0$ となる $\sigma' \in \mathrm{Gal}(\mathbf{Q}^{alg}/K)$ と $G(T) \in \mathbf{Z}[T]$ を探す

reduction map $A \longrightarrow B$ は $\mathrm{Tor}(A)$ 上 1 対 1 なので, $G(\sigma')|\mathrm{Tor}(B) = 0$ が成り立っていれば充分である. Lemma 5.0.9 より,

- B の good reductions p, l,
- $\sigma \in \mathrm{Gal}(K(\mathrm{Tor}_{p'}(B))/K)$ と $\tau \in \mathrm{Gal}(K(\mathrm{Tor}_p(B))/K)$
- $F_p(T), F_l(T) \in \mathbf{Z}[T]$: ともに 1 のべき乗根を解に持たない,

が存在して,

$$F_p(\sigma)|\mathrm{Tor}_{p'}(B) = 0 \text{ かつ } F_q(\tau)|\mathrm{Tor}_p(B) = 0$$

である.

Serre の結果より (Collected Papers, Vol IV, p. 33-34, p. 56-59)

$L = K(\mathrm{Tor}_{p'}(B)) \cap K(\mathrm{Tor}_p(B))$ は K の有限次ガロア拡大であり, $K(\mathrm{Tor}_{p'}(B))$ と $K(\mathrm{Tor}_p(B))$ は L 上線形無関連である.

ここで $m = [L : K]$ とおく.

$\alpha_1, \cdots, \alpha_{2d}$ を $F_p(T)$ の根, $\beta_1, \cdots, \beta_{2d}$ を $F_l(T)$ の根とし,

$$G(T) = \prod_{i=1}^{2d}(T - \alpha_i^m)(T - \beta_i^m)$$

とおく.

結論 : このとき σ^m と τ^m を拡大する $\sigma' \in \mathrm{Gal}(\mathbf{Q}^{alg}/L)$ が存在して,

1. $G(\sigma')|\mathrm{Tor}(B) = 0$ かつ,
2. $(\mathbf{Q}^{alg}, \sigma')$ を拡大する ACFA のどんなモデルにおいても, $\mathrm{Ker}(G(\sigma'))$ は B の one-based subgroup (modular subgroup) を定義する

3 つ目の道 : コンパクト性定理の応用 [Pillay]

コンパクト性定理を用いる方法もあるが, 詳しくは参考文献にある Pillay の論文を参照されたい.

7 Effective Bounds

1-基底群の定義可能部分集合は，有限個の剰余類のブール和になることが分かったが，何個の剰余類が必要なのだろうか．与えられた定義可能集合ごとに個数が変わることは用意に想像できるが，果たして個数の上限は存在するのだろうか．もし上限が存在するとして計算可能だろうか．Hrushovski は上限を計算する方法を明示している．$\mathrm{Tor}(A)$ と $\mathrm{Tor}'_p(A)$ について分かっているが，$\mathrm{Tor}(A)$ の場合は $\mathrm{Tor}'_p(A)$ に比べ，議論ははるかに複雑である．$\mathrm{Tor}'_p(A)$ の場合のみ論ずることにする．

7.1 $\mathrm{Tor}'_p(A)$ の場合

Theorem 6 X を定義可能集合とする．この X に対して

$$X \cap \mathrm{Tor}_{p'}(A) = \bigcup_{i=1}^{M} a_i + \mathrm{Tor}_{p'}(A_i)$$

となっているとする．ここで

- $d \leq \dim(A)$
- d_+ : A^3 の中で，A の加法を定義するグラフの次数

$$M \leq \left(\deg(X)^{2d+1}\ (d_+)^{2d^2\ (2d+1)\ (\log_2(1+q^{1/2})+1)^2}\right)^{2^d\ \dim(X)}$$

概略：

- $F(T) = \sum_{i=0}^{2d} m_i T^i,\ \ m_i \in \mathbf{Z}$
- $(\mathbf{Q}^a, \sigma) \subset (K, \sigma) \models \mathrm{ACFA}$
- $\tilde{S} = \mathrm{Ker}F(\sigma)$

$$S = \{(a_0, \ldots, a_{2d}) \in A^{2d+1} : \sum_{i=0}^{2d} [m_i]a_i = 0\}$$

とおく．

- $\sum |m_i| \leq (1+q^{1/2})^{2d}$ であり
- 2 以上の数 M を掛ける $= \log_2(M)(\log_2(M)+1)/2$ 回の足し算

よって，$\deg(S) \leq (d_+)^{2d^2(2d+1)(\log_2(1+q^{1/2})+1)^2}$

Z を $\tilde{S} \cap X$ のザリスキー閉包とすると

$$\deg(Z) \leq (\deg(X)^{2d+1}\deg(S))^{2^{2d\dim(X)}}$$

8 Tate-Voloch 予想

$\mathbf{Q}_p$ を p-進体，$\mathbf{C}_p$ を $\mathbf{Q}_p$ の代数的閉包の完備化とする．d_p を p-進距離とする．

Tate-Voloch 予想

G を $\mathbf{C}_p$ 上定義された準アーベル多様体，X を G の部分多様体とする．
自然数 N が存在して，

$$任意の P \in \mathrm{Tor}(G) に対して (P \notin X \Longrightarrow d_p(P, X) > N)$$

が成り立つ．

要するに，点 $P \in \mathrm{Tor}(G)$ に対して，P が X に入っていなければ X と P の間の p-進距離には下限が存在するという予想である．

Theorem (Tate and Voloch, 1996)

G がトーラスの時，予想は正しい．

Theorem (Hrushovski, 1996)

G が $\mathbf{Q}_p^{alg}$ 上定義されていて，good reduction を持ち，$\mathrm{Tor}_{p'}(G)$ に対して予想は正しい．

Theorem (Scanlon, 1998, 1999)

G が $\mathbf{Q}_p^{alg}$ 上定義されている時，予想は正しい．

T-V 予想．証明の概要 (Hrushovski)

- 1 のべき乗根を解に持たない $F[T] \in \mathbf{Z}[T]$ に対して，
  $\mathbf{C}_p$ の自己同型 σ が存在して
  $\mathrm{Tor}_{p'}(G) \subseteq \{a \in G(\mathbf{Q}_p^{alg}) : F(\sigma(a)) = 0\}$
- $a_0, \cdots, a_n, \cdots \in \mathrm{Tor}_{p'}(G)$，$\lim d_p(a_i, X) = 0$ とする．

目標：ほとんどの i について $a_i \in X$ を示す.

背理法で示す.

$\{i \in \mathbf{N} : a_i \in X\} \notin \mathcal{U}$ であるような $\mathbf{N}$ 上の non-principal untrafilter $\mathcal{U}$ が存在する.

$R = l^\infty(\mathbf{C}_p)$ を $\mathbf{C}_p$ の中の p-進ノルム有界な列全体とする．各 n に対して，$I_n = \{r \in R : \{i \in \mathbf{N} : |r(i)|_p \le p^{-n}\} \in \mathcal{U}\}$，とおき，$I = \bigcap I_n$ とすると，I は R のイデアルである.

$D = R/I$ は体であり，$\mathbf{C}_p$ を D に埋め込む. σ を D の自己同型に拡張する.

$a^* : D$ の中の $(a_0, \ldots, a_n, \ldots)$ の像とする．そうすると，$a \in G(D)$, $F(\sigma)(a^*) = 0$，$a^* \in X(D)$ である.

ここで $(D, \sigma) \prec (L, \sigma)$, generic diff. fields に移る.

$X(L) \cap \mathrm{Ker}(F(\sigma)) \subseteq \bigcup(c_i + B_i)$ （有限和）ただし，B_i は G の準アーベル部分多様体，$c_i + B_i \subset X$ である.

よって，$a^* \in c + B \subset X$，B は G の部分準アーベル多様体である.

$\pi : G \longmapsto G/B$ とすると，$\pi(a_i) \longrightarrow \pi(a^*)$ となる.

ほとんどすべての i について $\pi(a_i)$ の，剰余体における像は一致ので，reduction は $\mathrm{Tor}_{p'}(G/B)$ 上 1 対 1 である.

よって，ほとんどすべての i について　$\pi(a_i) = \pi(a^*)$ であり，ほとんどすべての i について $a_i \in c + B$ である．したがって，ほとんどすべての i について $a_i \in X$ である.

9 Drinfeld 加群

- K : 標数 $p > 0$ の代数的閉体，超越次数は正
- $\mathrm{End}_K(\mathbf{G}_a) = K$ 上定義された $\mathbf{G}_a$ の自己同型全体の環
- $\mathrm{End}_K(\mathbf{G}_a) \cong K[\phi_p]$
- T を K の超越元と考えて，$A = \mathbf{F}_p[T]$ を K の部分環と考える.

Definition

環準同型 $\varphi : A \longrightarrow \mathrm{End}_K(A)$ は,

$$\varphi(T) = \sum_{i=0}^{n} a_i \phi_p^i \implies a_0 = t \text{ かつ } a_n = 1$$

が成り立つ時，A 上の Drinfeld 加群 であると言う.

Theorem (Scanlon 1999)

- φ は Drinfeld 加群
- K^N を A-module と見なす
- X は K^N の部分多様体

$X \cap$(the A-torsion subgroup of K^N) $= \{x \in K^N : \varphi(a)(x) = 0\ (\exists 0 \neq a \in A)\}$ は K^N の有限個の部分代数群たちの A-torsion 部分群の剰余類の和集合である.

証明には, 標数 p の difference fileds のモデル理論 ($\mathbf{ACFA}_p$) の結果が必要である.

$\mathbf{ACFA}_p$ の Dichotomy Theorem の証明には, Zariski 幾何の議論が必要

最後に, どのような集合が Zarisiki 幾何を定義するかをまとめておく. いずれの場合も「次元定理」と呼ばれる定理が成り立つかどうかが鍵となっている.「次元定理」はまた, 対応するある種の環 (微分多項式環など) の Krull 次元を用いて証明される. 以下の例以外の新たな例を探すことは興味深い問題である.

Zariski 幾何 $\begin{cases} \text{diff. closed fields のランク 1 の集合} \\ \text{sep. closed fields のランク 1 の集合} \\ \text{difference fields のランク 1 の集合} \end{cases}$

参考文献

E. Hrushovski, *The Manin-Mumford conjecture and the model theory of difference fields*, Annals of Pure and Applied Logic, 112(2001) 43-115
(Received September 1995; accepted 17 April 2001)

E. Bouscaren, *Théorie des Modèles et Conjecture de Manin-Mimford d'après Ehud Hrushovski*, Séminaire Bourbaki, 52ème année, 1999-2000, n° 870

Z. Chatzidakis, *A Survey on the Model Theory of Difference Fields*, in **Model Theory, Algebra, and Geometry**, MSRI Publications vol 39, 2000

A. Pillay, *ACFA and the Manin-Mumford Conjecture*, in **Algebraic Model Theory**, Kluwer Academic Pub., 1997