ある種の群スキームのトーサーについて

On the torsors for some group schemes

情報セキュリティ科学専攻　戸田容平
Course of Information Security Science　Yohei Toda

1　導入

この研究の目的は, ある種の群スキームのトーサーを決定することである. 群スキームとは群を代数幾何学的に一般化したものであり, そのトーサーを決定することは, 群スキームに対する Galois の逆問題を解くことを意味する. トーサーについての古典的な結果としては Kummer 理論があり, それは次のようなものである.

n を 2 以上の整数, k を $\mathrm{ch}\, k \nmid n$ である体とし, k は 1 の原始 n 乗根を含むとする. このとき, 任意の n 次巡回拡大は, Kummer 完全列と呼ばれる完全列

$$1 \to \boldsymbol{\mu}_{p,k} \to \mathbb{G}_{m,k} \to \mathbb{G}_{m,k} \to 1$$

によって得られる.

F. Oort および J. Tate によって, 素数位数の有限群スキームが, 適切な a, b の選択のもとで $G_{a,b}$ という形の群スキームに同型であることが示されているが, L. G. Roberts [6] は基礎環が局所体の整数環の場合に, C. Andreatta および C. Gasbarri [1] は基礎環が完備離散付値環でその剰余体が正標数であり, かつ基礎環が b の $p-1$ 乗根を含む場合について, $G_{a,b}$ トーサーを決定している. 本研究ではこれらの先行研究とはまったく異なった手法および仮定のもとで $G_{a,b}$ トーサーを決定しており, すなわち, 円分捩れトーラスの概念を用いる方法である. 円分捩れトーラスの概念の一般論は B. Mazur, K. Rubin および A. Silverberg [4] によって与えられた. 彼らは, 1 次元代数的トーラスの Weil 制限のノルム写像たちの核の共通部分によって与えられる部分群スキームが円分捩れトーラスに同型であることを, 一般的な形で証明しており, 小出裕氏および關口力氏によって, 円分捩れトーラスが計算に援用できるような明示的な記述が与えられた.

本研究は, 彼らが与えた上記の同型を拡張して得られる完全列の存在を示すことから出発し, 円分捩れトーラスの自己準同型環を具体的に記述し, さらに, $\boldsymbol{\mu}_p$ をあるトーラスに埋め込み, それらのデサントにより得られる完全列を用いて, $G_{a,b}$ トーサーを決定する.

また, F. Oort および J. Tate による素数位数の有限群スキームの分類定理を素数冪位数の場合に拡張することにより, $\boldsymbol{\mu}_{p^l}$ のデサントのトーサーについてもある程度の結果を得ることができた. この研究をさらに押し進めて, 素数冪位数の有限群スキームの分類定理にまで発展させられることが期待される.

2　素数位数の群スキームの分類定理（Oort-Tate）

n を正の整数, m を n の Euler 関数の値, p を素数, ζ を 1 の原始 $p-1$ 乗根, G を σ_0 で生成される位数 n の巡回群, $\mathrm{Spec}\, B/\mathrm{Spec}\, A$ を G トーサー, $\mathbb{Z}_p$ を p 進整数環, A を Λ_p 代数とする. ただし, $\Lambda_p =$

$\mathbb{Z}[\zeta,(p(p-1))^{-1}]\cap\mathbb{Z}_p$. このとき, 任意の位数 p の A 上の群スキームは $G_{a,b}=\mathrm{Spec}\,(A[x]/(x^p-ax))$ に同型であり, 演算は,

$$m^*(x)=x\otimes 1+1\otimes x-\frac{b}{p-1}\sum_{i=1}^{p-1}U(i)x^i\otimes x^{p-i}$$

で与えられる. ここで, $a,b,\in A$, $U(i)\in A^\times$, $ab=\omega_p$ で, ω_p は p と $A^\times$ の元との積であり, $A^\times$ は A の可逆元全体からなる乗法群である.

3 円分捩れトーラス（Mazur-Rubin-Silverberg, 小出-關口）

$\mathbb{Z}[\zeta]$ の $\mathbb{Z}$ 上の基底 $\{1,\zeta,\zeta^2,\dots,\zeta^{m-1}\}$ への乗法による ζ の作用を表現する行列を I とおく. ベクトル $\boldsymbol{x}=(x_1,x_2,\dots,x_m)$ および行列 $M=(m_{ij})\in\mathrm{M}_{m\times l}(\mathbb{Z})$ に対し,

$$\boldsymbol{x}^M=\left(\prod_{j=1}^m x_j^{m_{j1}},\prod_{j=1}^m x_j^{m_{j2}},\dots,\prod_{j=1}^m x_j^{m_{jl}}\right)$$

と定義すると, $\mathbb{G}_{m,B}^m=\mathrm{Spec}\,B[x_1,x_1^{-1},x_2,x_2^{-1},\dots,x_m,x_m^{-1}]$ への G の作用を $\boldsymbol{x}^{\sigma_0}=\boldsymbol{x}^I$ で定義できる. この作用によって, $\mathbb{G}_{m,B}^m$ を A 上にデサントすることができるが, それを $\mathbb{G}(n)_A$ と書き, n 次の円分捩れトーラスと呼ぶ. 円分捩れトーラスの座標環は具体的に記述することができる. また, 円分捩れトーラスは,

$$\mathcal{T}(n)_A=\bigcap_{l|n}\mathrm{Ker}\left[\mathrm{Nm}_l:\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\to\mathrm{Res}_{B_l/A}\mathbb{G}_{m,B_l}\right]$$

で与えられる群スキームに同型である. ここで, Nm_l は B から $B_l=B^{\left\langle\sigma_0^{n/l}\right\rangle}$ へのノルム写像であり, $\mathrm{Res}_{B/A}$ は B から A への Weil 制限である.

4 円分分解

上記の同型 $\mathbb{G}(n)_A\cong\mathcal{T}(n)_A$ は, 次のような分解に拡張される.

定理 4.1. $k=\mathbb{F}_q$, $K=\mathbb{F}_{q^n}$ とおく. $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ を n の素因数分解とする. 整数 $1\le i_0<i_1<\cdots<i_s\le r$ に対し, $n_{i_0\cdots i_s}=n/p_{i_0}p_{i_1}\cdots p_{i_s}$, $M_{i_0i_1\cdots i_s}=\mathbb{F}_{q^{n_{i_0i_1\cdots i_s}}}$ とおく. このとき完全列

$$1\to\mathbb{G}(n)_k(k)\xrightarrow{\varepsilon}K^\times\xrightarrow{\partial^0}\prod_{i=1}^r M_i^\times\xrightarrow{\partial^1}\prod_{1\le i_0<i_1\le r}M_{i_0i_1}^\times\xrightarrow{\partial^2}\cdots\xrightarrow{\partial^{r-1}}M_{12\cdots r}^\times\to 1$$

が存在し, これを円分分解とよぶ. ここで, 準同型 ∂^i は,

$$\partial^0 x=\left(\mathrm{Nm}_{K^\times/M_1^\times}x,\mathrm{Nm}_{K^\times/M_2^\times}x,\cdots,\mathrm{Nm}_{K^\times/M_r^\times}x\right),$$
$$(\partial^s\boldsymbol{x})_{i_0i_1\cdots i_s}=\prod_{j=0}^s\left(\mathrm{Nm}_{M^\times_{i_0i_1\cdots\hat{i_j}\cdots i_s}/M^\times_{i_0i_1\cdots i_s}}x_{i_0i_1\cdots\hat{i_j}\cdots i_s}\right)^{(-1)^j}$$

で定義される.

定理 4.1 の証明の本質はノルム写像 $\mathbb{F}_{q^n} \to \mathbb{F}_q$ の全射性であるが, これは $(\operatorname{Spec} A)_{\mathrm{flat}}$ 上の層のノルム写像 $\operatorname{Res}_{B/A}\mathbb{G}_{m,B} \to \mathbb{G}_{m,A}$ の全射性に拡張され, これにより, 定理 4.1 は次のように一般化される.

定理 4.2. $(\operatorname{Spec} A)_{\mathrm{flat}}$ 上の群の層の列

$$1 \to \mathbb{G}(n)_A \to \operatorname{Res}_{B/A}\mathbb{G}_{m,B} \to \prod_{i=1}^{r} \left(\operatorname{Res}_{B_i/A}\mathbb{G}_{m,B_i}\right) \to \prod_{1\le i<j\le r} \left(\operatorname{Res}_{B_{ij}/A}\mathbb{G}_{m,B_{ij}}\right) \to \cdots \to 1$$

は完全. ただし $B_{i_0 i_1 \cdots i_s} = B^{\left\langle \sigma^{n_{i_0 i_1 \cdots i_s}} \right\rangle}$ である.

5 円分捩れトーラスの自己準同型環

円分捩れトーラス $\mathbb{G}(n)_A$ の自己準同型環は次で与えられる.

定理 5.1. $\operatorname{End}(\mathbb{G}(n)_A) \cong \mathbb{Z}[\zeta]$.

さらに, この定理 5.1 から次がしたがう.

命題 5.2. $\varphi \in \operatorname{End}(\mathbb{G}(n)_A)$ に対し, $\det\varphi = \operatorname{Nm}\varphi = \operatorname{ord}(\operatorname{Ker}\varphi)$. ただし, φ を表現する行列 M に対し $\det\varphi = \det M$, $\operatorname{Nm}\varphi = \operatorname{Nm} M$.

6 $G_{a,b}$ トーサー

$\mathfrak{p}$ を $\mathbb{Q}(\zeta)$ 上で完全分解する単項素イデアルとし, $\mathfrak{p} \cap \mathbb{Z} = (p)$ とする. 実際, $\mathfrak{p}$ は $p \equiv 1 \pmod{n}$ のとき, またそのときに限り完全分解する (cf. [9, Prop. 2.14.]). $n = p-1$, $\mathfrak{p} = (\theta)$, $X = \operatorname{Spec} A$ とおく. このとき, 完全列

$$1 \to \boldsymbol{\mu}_{p,B} \xrightarrow{\iota} \mathbb{G}_{m,B}^m \xrightarrow{\theta} \mathbb{G}_{m,B}^m \to 1$$

を A 上にデサントすることにより, 完全列

$$1 \to (\boldsymbol{\mu}_{p,B})^G \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 1$$

を得る. ここで, $x^n - b \in A[x]$ が既約, $ab = \omega_p$, $u = \sqrt[n]{b}$, $B = A[u]$ と仮定すると, $(\boldsymbol{\mu}_{p,B})^G \cong G_{a,b}$ となる. さらに, 長完全列

$$\begin{aligned} 1 \to H^0(X, G_{a,b}) &\xrightarrow{H^0(X,\iota)} H^0(X, \mathbb{G}(n)_A) \xrightarrow{H^0(X,\theta)} H^0(X, \mathbb{G}(n)_A) \\ &\xrightarrow{\partial} H^1(X, G_{a,b}) \xrightarrow{H^1(X,\iota)} H^1(X, \mathbb{G}(n)_A) \xrightarrow{H^1(X,\theta)} H^1(X, \mathbb{G}(n)_A) \end{aligned}$$

から, 非標準的な同型

$$H^1(X, G_{a,b}) \cong \operatorname{Coker} H^0(X,\theta) \times \operatorname{Ker} H^1(X,\theta)$$

を得る. $H^1(X, \mathbb{G}(n)_A)$ の情報は, 円分分解（定理 4.2）を用いて, 同様の手順で得られる.

素数 p の上の素イデアルが単項でない場合の結果は, 小出裕氏 [2] によって得られている.

$\boldsymbol{\mu}_{p^l,B}$ のデサントのトーサーについては, まず完全列

$$1 \to \boldsymbol{\mu}_{p^l,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\mathfrak{p}^l} \mathbb{G}_{m,B}^m \to 1,$$

を考える. ただし, p は奇素数とする. F. Oort および J. Tate は $\boldsymbol{\mu}_{p,B}$ の座標環を $(\mathbb{Z}/p\mathbb{Z})^\times$ の作用で固有空間に分けたが, ここでは $\boldsymbol{\mu}_{p^l,B}$ の座標環を $(\mathbb{Z}/p^l\mathbb{Z})^\times \cong \mathbb{Z}/p^{l-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ の 2 種類の作用によって固有空間に分けることで, $\boldsymbol{\mu}_{p^l,B}$ の座標環を書き換え, 完全列

$$1 \to \left(\boldsymbol{\mu}_{p^l,B}\right)^G \to \mathbb{G}(n)_A \xrightarrow{\mathfrak{p}^l} \mathbb{G}(n)_A \to 1$$

を用いて $(\boldsymbol{\mu}_{p^l,B})^G$ トーサーが決定される. ただし, $p-1$ 次のデサントは $G_{a,b}$ トーサーと同様の手法により, p^{l-1} 次のデサントは, $l=2$ の場合は關口-Oort-諏訪および Waterhouse による Kummer-Artin-Schreier 完全列

$$1 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{G}^{(\lambda)} \xrightarrow{\psi} \mathcal{G}^{(\lambda^p)} \to 1$$

を用い, $l \geq 3$ の場合は關口-諏訪による Kummer-Artin-Schreier -Witt 完全列

$$1 \to \mathbb{Z}/p^{l-1}\mathbb{Z} \to \mathcal{W}_{l-1} \to \mathcal{V}_{l-1} \to 1$$

を用いて記述される.

参考文献

[1] F. Andreatta and C. Gasbarri, *Torsors under some group schemes of order p^n*, Journal of Algebra 318 (2007), 1057–1067.

[2] Y. Koide, *On the Torsors for General Twisted Finite Group Schemes of Prime Order*, Preprint, 2012. (to appear in Journal of Algebra, Number Theory & Applications)

[3] Y. Koide and T. Sekiguchi, *On the Cyclotomic Twisted Torus*, Far East Journal of Mathematical Sciences, vol.72, No. 2 (2013), 201–224.

[4] B. Mazur, K. Rubin and A. Silverberg, *Twisting Commutative Algebraic groups,* Journal of Algebra 314 (2007), 419–438.

[5] F. Oort and J. Tate, *Group Schemes of Prime Order*, Annales Scientifiques de l'É.N.S., 4$^{\text{e}}$ série, tome 3 (1970), 1–21.

[6] L. G. Roberts, *The Flat Cohomology of Group Schemes of Rank p*, American Journal of Mathematics, The Johns Hopkins University Press, Vol.95, No.3 (1973), 688–702.

[7] T. Sekiguchi and Y. Toda, *On the cyclotomic twisted torus and some torsors*, International Journal of Pure and Applied Mathematics, 89, No.4 (2013), 461–482.

[8] Y. Toda, *On the torsors for group schemes of prime-power order*, International Journal of Pure and Applied Mathematics, 96, No.4 (2014), 407–425.

[9] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York Heidelberg Berlin (1982).