円分捻れトーラスに対する Kummer 理論
The Kummer Theory for Cyclotomic Twisted Tori

情報セキュリティ科学専攻　　小出　裕
Course of Information Security Science　Yu Koide

1　導入

本研究は，ある種の有限群スキーム $G_{a,b}$ に対するトーサーの決定が目的である．ここで X が $G_{a,b}$ に対するトーサーとは，大雑把に言って，$G_{a,b}$ の基礎スキーム上平坦位相の下で，X が $G_{a,b}$ に局所同型であることをいう．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である．通例の Galois の逆問題とは，与えられた有限群 G と体 k に対して，群 G が体 k のある Galois 拡大に対応する Galois 群であるかどうかという問題である．トーサーの決定に関する古典的な結果として，Kummer 理論がある．Kummer 理論とは，群スキーム $\mathbb{Z}/n\mathbb{Z}$ に対するスキーム X 上のトーサーをコホモロジーを用いて明示的に計算するものである．$X = \mathrm{Spec}\ k$ の場合は，よく知られた体上の Kummer 理論である．ここで，体上の Kummer 理論とは次のようなものである．n を 2 以上の正整数であり，$\mathrm{char}\ k \nmid n$ とし，ζ_n を 1 の原始 n 乗根とする．$\zeta_n \in k$ と仮定する．このとき，任意の n 次巡回拡大 K/k に対して，ある元 $t \in k$ が存在して，$K = k(s)$ をみたす．但し s は，方程式 $T^n - t = 0$ の解のひとつである．

そこで本研究では， Frans Oort と John Tate によって分類された素数位数 p の有限群スキーム $G_{a,b}$ に対するトーサーを決定する．ここで Frans Oort と John Tate による位数 p の有限群スキームの分類は，次のものである ([4]).

定理 1.1. $\Lambda_p = \mathbb{Z}\left[\zeta_{p-1}, \dfrac{1}{p(p-1)}\right] \cap \mathbb{Z}_p$ とする．ここで，$\mathbb{Z}_p$ を p 進整数環とする．A を Λ_p 代数とする．このとき，位数 p の A 上の有限群スキーム $G_{a,b}$ の同型類と三つ組 (L, a, b) の同型類と一対一対応する．ここで，L は階数 1 の射影 A 加群であり，また $a \in L^{\otimes(p-1)}$，$b \in L^{\otimes(1-p)}$ であって，$a \otimes b = \omega_p$ をみたす．但し，ω_p は素数 p と Λ_p のある可逆元との積である．

注意 1.1. 定理 1.1 における三つ組 (L, a, b) に対応する有限群スキーム $G_{a,b}$ の座標環は $A[x]/(x^p - ax)$ であり，その群演算は，$m^*(x) = x \otimes 1 + 1 \otimes x - \dfrac{b}{p-1}\displaystyle\sum_{i=1}^{p-1} U(i)x^i \otimes x^{p-i}$ である．但し，$U(i)$ は A のある可逆元とした．また Λ_p 代数 A が局所環のとき，三つ組 (L, a, b) と (L', a', b') が同型であるとは，$L \cong L'$ であり，ある可逆元 $u \in A$ があって $a' = u^{p-1}a$ かつ $b' = u^{1-p}b$ をみたすときをいう．

我々は，円分捻れトーラス（以下では CTT と略す）と呼ばれる有限群スキームを定義する ([3]). 特別な場合における CTT に対する Kummer 理論は，關口力氏と戸田容平氏により得られた ([7]). それは，次のようなものである．まずある整数環の主イデアルに対応する位数 p の自己準同型をもつ代数的トーラスに $\boldsymbol{\mu}_p$ を埋め込む．そしてその自己準同型によって，代数的トーラスと $\boldsymbol{\mu}_p$ の Galois デサントをとることで，CTT を係数とする 1 次元コホモロジーを計算するというものである．本研究の主結果は，關口力氏と戸田容平氏による結果を一般化したものである ([2]). つまり主イデアルに対応する自己準同型という仮定を必要とせず，CTT に対する Kummer 理論を展開した．

$G_{a,b}$ に対するトーサーの決定に関する先行研究としては，L. G. Roberts によるもの ([5]) と，F. Andreatta と C. Gasbarri によるもの ([1]) がある．前者は，群スキーム $G_{a,b}$ の定義環が局所体の整数環である場合にトーサーを決定している．後者は，群スキーム $G_{a,b}$ の定義環が完備離散付値環であり，剰余体の標数が p の場合であって，b が $\mathbb{F}_p$ の中で $p-1$ 乗根をもつという仮定の下でトーサーを決定している．

2　円分捻れトーラス（CTT)

本節では，円分捩じれトーラス (CTT) を定義する．そして CTT が，代数的トーラスの Weil 制限の間のすべてのノルム写像の核の共通部分がなす群スキームと自然に同型となることをみる．これは，關口力教授との共同研究の結果である．

n を正の整数とし，また $m=\phi(n)$ とする．但し ϕ は Euler 関数とした．さらに $\Phi_n(x)=x^m+a_1x^{m-1}+\cdots+a_m$ を円分多項式とする．よく知られていることだが，$\Phi_n(x)$ は，整数係数の多項式である．またさらに ζ を 1 の原始 n 乗根とし，$I\in M_m(\mathbb{Z})$ を $1,\zeta,\ldots,\zeta^{m-1}$ を整基底にもつ $\mathbb{Z}[\zeta]$ における ζ 倍の $\mathbb{Z}$ 加群 $\mathbb{Z}^m$ の標準基底に対する ζ の表現行列とする：

$$I=\begin{pmatrix}0&0&\cdots&0&-a_m\\1&0&\cdots&0&-a_{m-1}\\0&1&\cdots&0&-a_{m-2}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-a_1\end{pmatrix}.$$

ここで任意の $k,\ell\in\mathbb{Z}$ と任意のベクトル $\boldsymbol{x}=(x_1,x_2,\ldots,x_k)$ ，任意の行列 $M=(m_{ij})\in \mathrm{M}_{k,\ell}(\mathbb{Z})$ に対して，ベクトルの行列乗 $\boldsymbol{x}^M$ を次のように定義する：

$$\boldsymbol{x}^M=\left(\prod_{j=1}^k x_j^{m_{j1}},\prod_{j=1}^k x_j^{m_{j2}},\ldots,\prod_{j=1}^k x_j^{m_{j\ell}}\right).$$

$\mathrm{Spec}B/\mathrm{Spec}A$ を位数 n の巡回群 $G=\langle\sigma_0\rangle$ に対するトーサーとする．このとき，B 上の代数的トーラス $\mathbb{G}_{m,B}^m$ に次のように群 G の作用を定める：

$$\sigma_0:\begin{cases}B[x_1,x_2,\ldots,x_m,1/\prod_{i=1}^m x_i] & \xrightarrow{\sigma_0} B[x_1,x_2,\ldots,x_m,1/\prod_{i=1}^m x_i];\\ x=(x_1,x_2,\ldots,x_m) & \longmapsto x^{\sigma_0}=(x_1^\sigma,\ldots,x_m^\sigma):=x^I\\ b\in B & \longmapsto b^{\sigma_0}.\end{cases}$$

定義 2.1. B 上の代数的トーラス $\mathbb{G}_{m,B}^m$ の群 G による *Galois* 降下を $\mathbb{G}(n)_A$ と記し，n 次の**円分捩じれトーラス**（*cyclotomic twisted torus, CTT*）と呼ぶ*:*

$$\mathbb{G}(n)_A:=\mathbb{G}_{m,B}^m/G=\mathrm{Spec}\,B\left[x_1,x_2,\ldots,x_m,\frac{1}{\prod_{i=1}^m x_i}\right]^G.$$

注意 2.2. CTT の座標環は，明示的に求めることができる．

n を割り切る正の整数 ℓ に対して，$G_\ell=\left\langle\sigma_0^{n/\ell}\right\rangle\subset G$ とし，$B_\ell=B^{G_\ell}\subset B$ とする．このとき，n を割り切る各正整数 ℓ に対して，$\mathrm{Nm}_\ell:\mathrm{Res}_{B/A}(\mathbb{G}_{m,B})\to\mathrm{Res}_{B_\ell/A}(\mathbb{G}_{m,B_\ell})$. をノルム写像とする．ここで，$\mathrm{Res}_{B/A}\mathcal{G}$ は群スキーム $\mathcal{G}$ の Weil 制限である．そこで，$\mathrm{Res}_{B/A}\mathbb{G}_{m,B}$ の部分群スキーム $\mathcal{T}(n)_A$ を次のように定義する：

$$\mathcal{T}(n)_A:=\mathrm{Ker}\left((\mathrm{Nm}_\ell)_{\ell|n}:\mathrm{Res}_{B/A}\left(\mathbb{G}_{m,B}\right)\to\prod_{\ell|n}\mathrm{Res}_{B_\ell/A}\left(\mathbb{G}_{m,B_\ell}\right)\right).$$

このとき，$\mathcal{T}(n)_A$ は，CTT と自然に同型となる．

定理 2.1. A 上の群スキーム $\mathcal{T}(n)_A$ は，$\mathbb{G}(n)_A$ に自然に同型である．

定理 2.1 を証明する際，次の補題は重要である．

補題 2.1. 整数係数多項式 $A_1(X),\ldots,A_r(X)$ が存在して，$\Phi_n(X)=\sum_{i=1}^r A_i(X)F_i(X)$ をみたす．

3　特別な場合における CTT に対する Kummer 理論

本節では，關口力氏と戸田容平氏による，CTT に対する Kummer 理論を紹介する ([7]).

p を素数，$n = p - 1$ とし，ζ を 1 の原始 n 乗根とする．このとき，代数体 $\mathbb{Q}(\zeta)/\mathbb{Q}$ の整数環 $\mathbb{Z}[\zeta]$ の素イデアルで $p \in \mathbb{Z}$ の上にあるものを $\mathfrak{p}$ とする．ここで $\mathfrak{p}$ が主イデアルであると仮定し，$\theta \in \mathbb{Z}[\zeta]$ を $\mathfrak{p}$ の生成元とする．$\mathbb{Z}[\zeta] \subset \mathrm{End}(\mathbb{G}^m_{m,B})$ ([3]) であることより，$\theta \in \mathrm{End}(\mathbb{G}^m_{m,B})$ とみなすことができるので，短完全列

$$1 \longrightarrow \boldsymbol{\mu}_{p,B} \longrightarrow \mathbb{G}^m_{m,B} \xrightarrow{\theta} \mathbb{G}^m_{m,B} \longrightarrow 1 \tag{1}$$

を得る．ここで，$\deg \theta = p$ であることに注意する．$b \in A$ の n 乗根 u とし，$B = A[u]$ と仮定する．このとき，有限群スキーム $G_{a,b}$（定理 1.1）に関して，$\left(\boldsymbol{\mu}_{p,B}\right)^G \cong G_{a,b}$ となることが確かめられている．そこで Galois 降下によって，短完全列 (1) より次の CTT に対する Kummer 列を得る：

$$1 \longrightarrow G_{a,b} \longrightarrow \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \longrightarrow 1.$$

さらにこの Kummer 列から次のコホモロジーの長完全列を得る：

$$\begin{aligned} 1 \longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, G_{a,b}) &\longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^0(\theta)} \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial^0} \mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b}) &\longrightarrow \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^1(\theta)} \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial^1} &\cdots . \end{aligned}$$

これより，次のコホモロジー群に関する同型が得られる：

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

ここで上の同型は，具体的な元の対応が得られていることに注意する．よって，$\mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b})$ が計算できるためには，$\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A)$ を求めなければならない．これは，Cyclotomic 分解という CTT に関する複体により計算できることが，關口力氏と戸田容平氏により示されている．

4　一般の場合における CTT に対する Kummer 理論

本節では，主結果である關口力氏と戸田容平氏による結果の一般化について述べる．記号は，前節までと同様とする．$\mathfrak{a}$ を整数環 $\mathbb{Z}[\zeta]$ のイデアルとする．よく知られたことであるが，$\xi, \eta \in \mathbb{Z}[\zeta]$ が存在して，$\mathfrak{a} = (\xi, \eta)$ をみたす．このときイデアル $\mathfrak{a}$ に対応する準同型 $\psi_{\mathfrak{a}}$ を次のように定義する：

$$\begin{aligned} \psi_{\mathfrak{a}} : \mathbb{G}(n)_A &\longrightarrow \mathbb{G}(n)_A \times \mathbb{G}(n)_A \\ \boldsymbol{x} &\longmapsto (\boldsymbol{x}^{\xi(I)}, \boldsymbol{x}^{\eta(I)}) \end{aligned}$$

ここで $\xi(I)$ と $\eta(I)$ は，それぞれ ξ と η の表現行列とした．$\mathbb{G}(n)_A[\mathfrak{a}] := \mathrm{Ker}(\psi_{\mathfrak{a}} : \mathbb{G}(n)_A \to \mathbb{G}(n)_A \times \mathbb{G}(n)_A)$ とする．このとき，我々は次の定理を得た．

定理 4.1. $\mathbb{Z}$ 上不分岐な素イデアルからなる各イデアル $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ に対して，

$$|\mathbb{G}(n)_A[\mathfrak{a}]| = \mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\, \mathfrak{a}.$$

が成り立つ．

注意 4.1. $\mathbb{G}(n)_A[\mathfrak{a}]$ は，イデアル $\mathfrak{a}$ の生成元の取り方に依存せずに定まる．

$p \in \mathbb{Z}$ の上にある整数環 $\mathbb{Z}[\zeta]$ の素イデアルのひとつを $\mathfrak{p}$ とする．このとき $\theta \in \mathbb{Z}[\zeta]$ が存在して，$\mathfrak{p} = (p, \theta)$ をみたす．

定理 4.2. 上のように定めた各イデアル $\mathfrak{p} = (p, \theta)$ に対して，次のような $(\operatorname{Spec} B)_{\mathit{flat}}$ 上の群層の列が完全となるように準同型 ψ をとることができる：

$$1 \longrightarrow \boldsymbol{\mu}_{p,B} \longrightarrow \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \xrightarrow{\psi} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m,$$

但し $\psi_{\mathfrak{p}}(\boldsymbol{x}) = (\boldsymbol{x}^p, \boldsymbol{x}^\theta)$ とし，$\psi(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}^\beta \boldsymbol{v}^{-\alpha}, \boldsymbol{u}^{\beta'} \boldsymbol{v}^{-\alpha'})$ とした．

注意 4.2. $\alpha, \alpha', \beta, \beta'$ は，$\mathbb{Z}[\zeta]$ の元であって，イデアル $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ から自然に得られる．

定理 4.2 から次の短完全列が得られる：

$$1 \to \boldsymbol{\mu}_{p,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \operatorname{Ker}(\psi : \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \to \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m) \to 1. \tag{2}$$

ここで $\operatorname{Ker}(\psi : \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \to \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m)$ の定義方程式は，明示的に求めることができることに注意する．このとき，Galois 降下により，この短完全列は，次のような Kummer 列となる：

$$1 \longrightarrow G_{a,b} \longrightarrow \mathbb{G}(n)_A \xrightarrow{\psi_{\mathfrak{p}}} \overline{\operatorname{Ker} \psi} \longrightarrow 1,$$

ここで，$\overline{\operatorname{Ker} \psi}$ は $\operatorname{Ker} \psi$ の Galois 降下とした．この Kummer 列を用いて，關口力氏と戸田容平氏の結果と同様に $G_{a,b}$ に対するトーサーを決定することができる．

最後に，本結果は $n|(p-1)$ として得られたトーサーの計算の系として得られたものであることを言及しておく．また 2 節で紹介した群スキーム $\mathcal{T}(n)_A$ は，暗号理論で応用されている ([6])．2 節の同型定理を用いて，CTT 上でも公開鍵暗号を構成することができると考えられる．

参考文献

[1] F.Andreatta and C.Gabbarri, *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), pp.201-224.

[4] F.Oort and J.Tate, *Group Schemes of Prime Order*, Annales Scientifiques de l'É.N.S., 4^e série, tome3, 1970, P.1-21.

[5] L.G.Roberts, *The Flat Cohomology of Group Schemes of Rank p*, American Journal of Mathematics, Vol.95, No.3(Autumn, 1973), pp.688-702.

[6] K. Rubin and A. Silverberg, *Torus-based cryptography*, in *Advances in Cryptography-CRYPTO 2003*. Lect. Notes in Comp. Sci. vol.2729(Springer, Berlin, 2003), pp.349-365.

[7] T.Sekiguchi and Y.Toda, *On the cyclotomic twisted torus and some torsors*, Preprint, 2012.