円分捩れトーラスの自己準同型環と分解について

On the endomorphism ring and a resolution of a cyclotomic twisted torus

数学専攻　戸田容平
Yohei Toda

概要

この論文は, 關口力教授との共同研究である. 小出裕氏および關口力教授は [1] において, 円分捩れトーラスと, 1 次元代数的トーラスの Weil restriction のノルム写像の核の共通部分によって与えられる部分群スキームとの間の同型を与えている. ここでは, 1 次元代数的トーラスの Weil restriction のノルム写像を拡張して得られる完全列の存在を示し, さらに円分捩れトーラスの自己準同型環を具体的に記述する.

1　導入

この論文を通して, 特に断りのない限りは, n を正の整数, $m = \phi(n)$ をそのオイラー関数の値, G を, σ を生成元とする位数 n の巡回群とする. B/A を G-トーサーとする. ただし, B は自由 A 加群であると仮定する. ζ を 1 の原始 n 乗根とし, I を, ζ の $\mathbb{Z}[\zeta]$ への乗法による作用を表現する行列とする. すると, $(x_1, \cdots, x_m)^\sigma := (x_1, \cdots, x_m)^I$ によって $B[x_1, \cdots, x_m, 1/\prod_{i=1}^m x_i]$ 上に, Galois 作用によって B 上に, 標準的な G-作用を定義することができる. この G-作用によって, トーラス $\mathbb{G}_{m,B}^m$ を A 上に descent することができるが, これを円分捩れトーラスとよび, $\mathbb{G}(n)_A$ と書くとこにする. このとき, 円分捩れトーラスは n 個の G-不変であるパラメータ $\xi_1, \xi_2, \cdots, \xi_n$ とイデアル $\mathfrak{A}$ によって, 次のように具体的に記述することができる;

$$\mathbb{G}(n)_A = \mathrm{Spec} A[\xi_1, \xi_2, \cdots, \xi_n]/\mathfrak{A}.$$

(cf. [1, Th. 4.1.].) 円分捩れトーラスは標準的に, ノルム写像の核の共通部分に同型である. 実際, n の正の約数 ℓ に対し $B_\ell := B^{<\sigma^{n/\ell}>} \subseteq B$ と定義し,

$$\mathrm{Nm}_\ell : \prod_{B/A} \mathbb{G}_{m,B} \to \prod_{B_\ell/A} \mathbb{G}_{m,B_\ell}$$

を B から B_ℓ へのノルム写像とすると, 群スキーム

$$\mathcal{T}(n)_A := \bigcap_{\ell|n} \mathrm{Ker}(\mathrm{Nm}_\ell) \subseteq \prod_{B/A} \mathbb{G}_{m,B}$$

は円分捩れトーラス $\mathbb{G}(n)_A$ に他ならない.(cf. [1, Th. 6.1.].)

2 円分分解

ここで, 後の定理で大事な役割を担う, ノルム写像の全射性について記しておく.

補題 2.1. q を素数の冪とする. このとき, ノルム写像

$$\mathrm{Nm} : \mathbb{F}_{q^n} \to \mathbb{F}_q$$

は全射である.

これは, $\mathbb{F}_{q^n}$ の原始元のノルムが $\mathbb{F}_q$ の原始元となることからしたがう. ここから先は, 特に断りがない限り, $\mathbb{F}_q$, $\mathbb{F}_{q^n}$ をそれぞれ k, K と書くことにする. 小出裕氏および關口力教授は [1] において, 円分捩れトーラスと, 1 次元代数的トーラスの Weil restriction のノルム写像の核の共通部分によって与えられる部分群スキームとの間の同型を与えているが, このノルム写像の先はどのような形で与えられるかという問題に対する答えが次である.

定理 2.2. $n = p_1^{e_1} \cdots p_r^{e_r}$ を n の素因数分解とする. 整数 $1 \leq i_0 < \cdots < i_s \leq r$ に対し, $n_{i_0 \cdots i_s} = n/p_{i_0} \cdots p_{i_s}$, $M_{i_0 \cdots i_s} = \mathbb{F}_{q^{n_{i_0 \cdots i_s}}}$ とおく. このとき次の完全列が存在し, これを円分分解とよぶ;

$$\begin{aligned} 1 \to \mathbb{G}(n)_k(k) \xrightarrow{\varepsilon} K^\times \xrightarrow{\partial^0} \prod_{i=1}^{r} M_i^\times \xrightarrow{\partial^1} \prod_{1 \leq i_0 < i_1 \leq r} M_{i_0 i_1}^\times \xrightarrow{\partial^2} \cdots \\ \cdots \xrightarrow{\partial^{r-2}} \prod_{i=1}^{r} M_{1 \cdots \hat{i} \cdots r}^\times \xrightarrow{\partial^{r-1}} M_{1 \cdots r}^\times \to 1. \end{aligned}$$

ただし $K^\times$ は K の可逆元からなる乗法群であり, 準同型 ∂^i は $x \in K$ に対し

$$\partial^0 x = \left(\mathrm{Nm}_{K^\times / M_1^\times} x, \cdots, \mathrm{Nm}_{K^\times / M_r^\times} x \right),$$

$\mathbf{x} = (x_{i_0 \cdots i_{s-1}})_{1 \leq i_0 < \cdots < i_{s-1} \leq r} \in \displaystyle\prod_{1 \leq i_0 < \cdots < i_{s-1} \leq r} M_{i_0 \cdots i_{s-1}}^\times$ に対し

$$(\partial^s \mathbf{x})_{i_0 \cdots i_s} = \prod_{j=0}^{s} \left(\mathrm{Nm}_{M_{i_0 \cdots \hat{i_j} \cdots i_s}^\times / M_{i_0 \cdots i_s}^\times} x_{i_0 \cdots \hat{i_j} \cdots i_s} \right)^{(-1)^j}$$

で定義される.

上記の列が複体であることは明らかである. 証明は n の素因数の個数 r に関する帰納法によるが, $r = 2$ の場合を証明すれば, 一般の r の場合は同様の手法で証明できる. 証明の本質的な部分はノルムの全射性と, 次の補題である.

補題 2.3. $\Phi_n(X)$ を円分多項式とし, $F_i(X) = (X^n - 1)/(X^{n_i} - 1)$ とおく. このとき, 多項式 $A_1(X), \cdots, A_r(X) \in \mathbb{Z}[X]$ が存在して, $\Phi_n(X) = \sum_{i=1}^{r} A_i(X) F_i(X)$ を満たす. *(cf. [1, Lem. 6.4., Prop. 7.4.]).*

一般の r (ただし $s+1 \neq r-1$) の場合は, $\mathbf{x} = (x_{i_0 \cdots i_s})_{1 \leq i_0 < \cdots < i_s \leq r} \in \mathrm{Ker}\partial^{s+1}$ に対し

$$\mathbf{x}' = (x_{i_0 \cdots i_s})_{1 \leq i_0 < \cdots < i_s \leq r-1}$$

を考えることで帰納法の仮定が適用できる.

列の最後の部分の完全性 $\left(\mathrm{Ker}\partial^{r-1} \subseteq \mathrm{Im}\partial^{r-2}\right)$ については, $\mathbf{x} = (x_{\hat{1}}, x_{\hat{2}}, \cdots, x_{\hat{r}}) \in \mathrm{Ker}\partial^{r-1}$ に対し, $z_2, \cdots, z_r \in K^\times$ を $x_{\hat{i}} = \mathrm{Nm}_{K^\times/M_{\hat{i}}} z_i$ となるように選び,

$$\mathbf{x}' = \left(x_{\hat{1}}, \prod_{j=2}^{r} \left(\mathrm{Nm}_{K^\times/M_{\hat{2}}^\times} z_j \right)^{(-1)^j} \right)$$

を考えることで帰納法の仮定が適用できる.

定理 2.2 の証明の重要なポイントのひとつが

$$\mathrm{Nm} : K = \mathbb{F}_{q^n} \to k = \mathbb{F}_q$$

の全射性であったが, この全射性から, flat site $(A)_{\mathrm{flat}}$ 上の層のノルム写像

$$\mathrm{Nm} : \prod_{B/A} \mathbb{G}_{m,B} \to \mathbb{G}_{m,A}$$

を得る. これにより, 定理 2.2 と同様の議論によって次の定理を得る.

定理 2.4. $(A)_{\mathrm{flat}}$ 上の群の層の列

$$1 \to \mathbb{G}(n)_A \xrightarrow{\varepsilon} \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{\partial^0} \prod_{i=1}^{r} \left(\prod_{B_i/A} \mathbb{G}_{m,B_i} \right) \xrightarrow{\partial^1} \prod_{1 \leq i_0 < i_1 \leq r} \left(\prod_{B_{i_0 i_1}/A} \mathbb{G}_{m,B_{i_0 i_1}} \right) \xrightarrow{\partial^2} \cdots \xrightarrow{\partial^{r-1}} \prod_{B_{1\cdots r}/A} \mathbb{G}_{m,B_{1\cdots r}} \to 1$$

は完全. ただし $B_{i_0 \cdots i_s} := B^{<\sigma^{n i_0 \cdots i_s}>}$ である.

3 円分振れトーラスの自己準同型環

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

定理 3.1. 次の標準的な同型

$$\mathrm{End}\left(\mathbb{G}(n)_A\right) \cong \mathbb{Z}[\zeta]$$

が存在する.

$\mathrm{End}\left(\mathbb{G}(n)_A\right) \supseteq \mathbb{Z}[\zeta]$ は明らかなので, 逆の包含関係が本質的である. 証明は, $\varphi \in \mathrm{End}\left(\mathbb{G}(n)_A\right)$ が行列 $M = (b_{ij}) \in \mathrm{M}_m(\mathbb{Z})$ で表現されて $MI = IM$ を満たすことから強引に計算する. 実際, この行列 M は $c_1, \cdots, c_m \in \mathbb{Z}$ が存在して

$$M = \sum_{i=1}^{m} c_i I^{i-1}$$

となる.

さらに, この定理 3.1 から次がしたがう.

命題 3.2. $\varphi \in \mathrm{End}(\mathbb{G}(n)_A)$ に対し

$$\left|\det\varphi\right| = \left|\mathrm{Nm}\varphi\right| = \mathrm{ord}(\mathrm{Ker}\varphi).$$

ただし, φ を表現する行列 M に対し $\det\varphi = \det M$, $\mathrm{Nm}\varphi = \mathrm{Nm}M$.

証明は, Frobenius の定理から $\det M = \mathrm{Nm}M$ がしたがい, 正則行列 $J, J' \in \mathrm{GL}_m(\mathbb{Z})$ が存在して JMJ' が体格行列となることから $\left|\det M\right| = \mathrm{ord}(\mathrm{Ker}\varphi)$ がしたがう.

4 今後の展望

以上の結果から, 円分捩れトーラスのコホモロジーがある程度計算され, さらに, ある種の有限群スキームに関するトーサーを決定することが期待される.

参考文献

[1] Y. Koide and T. Sekiguchi, *On The Cyclotomic Twisted Torus*, Preprint, 2011.

[2] K. Rubin and A. Silverberg, *Torus-Based Cryptography*, Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, Volume 2729, 349–365.

[3] J. S. Milne, *Étale Cohomology*, Princeton University Press.