SUT Journal of Mathematics
Vol. 55, No. 2 (2019), 95–108

Algebraic extensions attached to algebraic tori of relative norm

Masanari Kida

(Received March 10, 2019)

Abstract. We prove a Kummer-type duality theorem over certain fields without roots of unity by using algebraic tori of relative norm.

AMS 2010 *Mathematics Subject Classification.* 11R32, 12F10.

Key words and phrases. Kummer theory, cyclic extension, algebraic torus.

§1. Main theorem

Let G be a commutative algebraic group defined over a field k. We fix a separable closure $\overline{k}$ of k once for all and assume that all separable extensions of k lie inside $\overline{k}$. Suppose that there is a separable isogeny

$$\lambda \ : \ G \longrightarrow G \tag{1.1}$$

defined over k. From the associated exact sequence

$$1 \longrightarrow \ker(\lambda) \longrightarrow G \xrightarrow{\lambda} G \longrightarrow 1,$$

we have an induced exact sequence of Galois cohomology groups:

$$1 \longrightarrow G(k)/\lambda G(k) \longrightarrow \mathrm{H}^1(k, \ker(\lambda)) \longrightarrow \mathrm{H}^1(k, G)[\lambda].$$

Here we abbreviate $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), V(\bar{k}))$ as $\mathrm{H}^1(k, V)$ for any algebraic group V defined over k. Assume further that the points in the kernel of λ are k-rational:

$$\ker(\lambda)(\overline{k}) = \ker(\lambda)(k) \tag{1.2}$$

and that we have a weaker version of Hilbert's theorem 90:

$$\mathrm{H}^1(k, G)[\lambda] = 1, \tag{1.3}$$

then we have a Kummer duality

$$G(k)/\lambda G(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{k}/k), \ker(\lambda)(\overline{k})), \tag{1.4}$$

where the right hand side is the group of continuous homomorphisms. The isomorphism (1.4) is induced by the connecting homomorphism, which is explicitly given by the following way: For $P \in G(k)$, we choose $Q \in G(\overline{k})$ such that $\lambda(Q) = P$ and define a homomorphism $\chi_P \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{k}/k), \ker(\lambda)(\overline{k}))$ corresponding to P by $\chi_P(\tau) = Q^{\tau-1}$ for $\tau \in \mathrm{Gal}(\overline{k}/k)$.

In this framework, the classical Kummer theory is recovered by taking $G = \mathbb{G}_{m,\,k}$ and the m-th power map for λ if k contains the group of m-th roots of unity and the characteristic of k is prime to m.

If we have the Kummer duality (1.4), then all cyclic extensions of degree m over k are of the form $k(\lambda^{-1}(P))$ with some $P \in G(k)$. Since the Galois action on $\lambda^{-1}(P)$ is given by the multiplication by the elements in $\ker\lambda$, we can expect that their arithmetic properties such as decomposition law of prime ideals are easy to describe.

In our previous papers [4] and [6], we considered the case where G is an algebraic torus and proved Kummer dualities over certain fields without roots of unity. To be more specific, we used the Weil restriction of multiplicative group in [6] and norm algebraic tori in [4].

The aim of this paper is to extend the results in [4] and to prove a Kummer duality for algebraic tori of relative norm. An advantage of this duality theorem over the previous theorems is that we need algebraic varieties of smaller dimension to parameterize cyclic extensions over a base field. For example, we can show that all quintic cyclic extensions over the field of rational numbers are obtained as "Kummer extensions" associated to certain 2-dimensional rational algebraic torus (see Example 4.3). This dimension 2 agrees with the known minimal number of parameters we need to parameterize such cyclic quintic extensions (the essential dimension for C_5 in the language of [3]). Moreover, the required isogeny in λ in (1.1) is easier to find in our current setting than in the previous ones.

Throughout this paper, we use the following notation: for a positive integer $n > 1$ and a positive divisor s of n, let $R(n, s)$ be the set of positive divisors of n which do not divide s:

$$R(n, s) = \{d \in \mathbb{Z}_{>0} : d \mid n,\ d \nmid s\}. \tag{1.5}$$

For $r \in R(n, s)$, we denote by ζ_r a primitive r-th root of unity.

Our main theorem is as follows.

Theorem 1.1. *Let m be a positive integer greater than 1 and n a positive divisor of $\varphi(m)$ which is prime to m and s a positive divisor of n.*

Suppose that there exist a polynomial

$$\mathscr{P}(t) = c_1 + c_2 t + \cdots + c_{n-s-1} t^{n-s-1} \in \mathbb{Z}[t] \tag{1.6}$$

of degree less than or equal to $n-s-1$, a subset R of $R(n,s)$, and a set of pairwise coprime integers $\{m_r \mid r \in R\}$ indexed by R satisfying the following properties:

- $n = \mathrm{lcm}\{r \mid r \in R\}$;
- $\prod_{r \in R} m_r = m$;
- *if $r \in R$, then there is an isomorphism*

$$\mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \cong \mathbb{Z}/m_r\mathbb{Z}; \tag{1.7}$$

- *if $r \in R(n,s) \backslash R$, then*

$$\mathscr{P}(\zeta_r) \in \mathbb{Z}[\zeta_r]^\times. \tag{1.8}$$

Let k be a field of characteristic prime to m such that the ring isomorphisms (1.7) *induce a group isomorphism*

$$\nu_k \ : \ \mathrm{Gal}(k(\zeta_m)/k) \xrightarrow{\sim} \langle \zeta_r \bmod \ \mathscr{P}(\zeta_r) \mid r \in R \rangle. \tag{1.9}$$

Let $K = k(\zeta_m)$ and M an intermediate field of K/k such that $[M:k] = s$.

Under these conditions, there exists a cyclic self-isogeny λ of degree m on the algebraic torus

$$T_s := \ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m)$$

for which we have $\ker\lambda \cong \mathbb{Z}/m\mathbb{Z}$ with trivial Galois action and the exact sequence attached to the isogeny λ

$$1 \longrightarrow \ker\lambda \longrightarrow T_s \xrightarrow{\lambda} T_s \longrightarrow 1$$

induces the Kummer duality

$$\kappa_k \ : \ T_s(k)/\lambda T_s(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda(\bar{k})). \tag{1.10}$$

The algebraic torus T_s is defined as the kernel of the induced map from the relative norm map $N_{K/M} : K^\times \longrightarrow M^\times$. Thus we call an algebraic torus isomorphic to T_s for some $K/M/k$ an algebraic torus of relative norm. When $s = 1$, we have $M = k$ and T_1 is the norm torus $R^{(1)}_{k_c/k}\mathbb{G}_m$. The Kummer duality

for $R^{(1)}_{k_c/k}\mathbb{G}_m$ proved in [4] readily follows from our theorem. Even in this case, we relax conditions for the existence of required isogeny by introducing the set R. This set R enables us to find explicit examples easier than before (see examples in Section 4). Since

$$\dim T_s = n - s \leq n - 1 = \dim R^{(1)}_{K/k}\mathbb{G}_m < \dim R_{K/k}\mathbb{G}_m,$$

our theorem requires a smaller variety to parameterize all cyclic extensions over k.

The rest of the paper is organized as follows. We shall study the endomorphisms of T_s in the next section. The proof of the main theorem will be given in Section 3. In Section 4 we give some explicit examples.

Remark 1.2. In proving the corresponding main theorem in our previous paper [6], we did need the condition $(m, n) = 1$, which was not explicitly mentioned in the paper. In this occasion, we include this correction here.

§2. The endomorphism ring of T_s

In this section, we compute endomorphisms of T_s in a general setting.

Let K/k be a cyclic extension of degree n with Galois group $G = \mathrm{Gal}(K/k)$ generated by τ. Let s be a divisor of $[K : k]$ and M the fixed field of $\langle \tau^s \rangle$. We have

$$[M : k] = s \text{ and } \mathrm{Gal}(K/M) = \langle \tau^s \rangle.$$

Let $d = n/s$. As before we define

$$T_s = \ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m),$$

where $N_{K/M}$ is the map induced by the relative norm map $x \mapsto \prod_{i=0}^{d-1} \tau^{si} x$. The algebraic torus T_s is defined over k and splits over K. The dimension of T_s is $n - s$.

The character module of an algebraic k-torus T splitting over K is $\widehat{T} = \mathrm{Hom}_{K\text{-gr}}(T \times_k K, \mathbb{G}_{m,K})$ by definition. The character module $\widehat{T}$ is a free $\mathbb{Z}$-module of rank $\dim T$ on which $\mathrm{Gal}(K/k)$ acts.

Let $G = \mathrm{Gal}(K/k) = \langle \tau \rangle$ and $H = \mathrm{Gal}(K/M) = \langle \tau^s \rangle$. We start with the exact sequence

$$1 \longrightarrow I_{G/H} \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon_{G/H}} \mathbb{Z}[G/H] \longrightarrow 1,$$

where $\varepsilon_{G/H}$ is the augmentation map defined by

$$\sum_{i=1}^{n} a_i \tau^i \mapsto \sum_{i=0}^{s-1} \left(\sum_{\tau^j \in \tau^i H} a_j \right) \tau^i H$$

and $I_{G/H}$ is the kernel of $\varepsilon_{G/H}$. The inner sum is taken for all j such that $\tau^j \in \tau^i H$. The dual of the sequence is

$$1 \longrightarrow \mathrm{Hom}(\mathbb{Z}[G/H], \mathbb{Z}) \xrightarrow{v} \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z}) \longrightarrow \mathrm{Hom}(I_{G/H}, \mathbb{Z}) \longrightarrow 1,$$

which is also exact. The map v is given by

$$\tau^i H \mapsto \tau^i(1 + \tau^s + \cdots + \tau^{n-s})$$

under the canonical identifications

$$\mathrm{Hom}(\mathbb{Z}[G/H], \mathbb{Z}) \cong \mathbb{Z}[G/H] \quad \text{and} \quad \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z}) \cong \mathbb{Z}[G].$$

Since this map v is the dual of

$$N_{K/M} \ : \ R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m,$$

we obtain

$$\widehat{T_s} \cong \mathrm{Hom}(I_{G/H}, \mathbb{Z})$$

as G-modules. The $n - s$ elements

$$e_{ij} = \tau^i(\tau^{js} - \tau^{(j-1)s}) \ (i = 0, \ldots, s-1, j = 1, \ldots, d-1)$$

form a basis of $I_{G/H}$. By computing the dual action of τ on the basis

$$(e_{01}, \ldots, e_{s-1,1}, \ldots, e_{0,d-1}, \ldots, e_{s-1,d-1}),$$

we obtain the following representation matrix with respect to the canonical dual basis:

$$S = \begin{bmatrix} \mathbf{0}_{s-1} & -1 & \mathbf{0}_{s-1} & -1 & \cdots & \mathbf{0}_{s-1} & -1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & O & & \\ & & & \ddots & & & \\ & O & & & \ddots & & \\ & & & & & 1 & 0 \end{bmatrix}, \tag{2.1}$$

where $\mathbf{0}_{s-1}$ is the $(s-1)$-dimensional row zero vector.

Proposition 2.1. *The endomorphism ring of the character module $\widehat{T_s}$ is isomorphic to the polynomial ring in S with coefficients in $\mathbb{Z}$:*

$$\mathrm{End}_{\langle\tau\rangle}(\widehat{T_s}) \cong \mathbb{Z}[S].$$

We shall first show that the characteristic polynomial of S is separable.

Lemma 2.2. *The characteristic polynomial of S is*

$$x^{n-s} + x^{n-2s} + \cdots + x^s + 1 = \prod_{r \in R(n,s)} \Phi_r(x),$$

where $R(n,s)$ is defined by (1.5) *and Φ_r is the r-th cyclotomic polynomial.*

Proof. The first expression follows from a general formula

$$\begin{vmatrix} x & a_{k-1} & a_{k-2} & \cdots & a_1 & a_0 \\ -1 & x & 0 & \cdots & & 0 \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ 0 & & & & -1 & x \end{vmatrix} = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0,$$

which is deduced from the cofactor expansion by the first row of the matrix.

As for the second expression, since

$$x^n - 1 = \prod_{r|n} \Phi_r(x) \text{ and } x^s - 1 = \prod_{r|s} \Phi_r(x),$$

we have

$$x^{n-s} + x^{n-2s} + \cdots + x^s + 1 = \frac{x^n - 1}{x^s - 1} = \prod_{r|n,\ r\nmid s} \Phi_r(x).$$

This completes the proof of the lemma. □

From Lemma 2.2 it follows that the characteristic polynomial is separable. Now we are ready to prove Proposition 2.1.

Proof of Proposition 2.1. We fix the basis of $\widehat{T}_s$ chosen in the above. Then the matrices corresponding to the G-endomorphisms of the character module agree with the matrices which commute with S. We have shown that the characteristic polynomial of S is separable. In this situation, it is more or less known that such matrices are polynomials in S. This completes the proof of the proposition. □

By Proposition 2.1, for an endomorphism Λ of $\widehat{T}_s$, we can find a polynomial

$$\mathscr{P}(t) = c_1 + c_2 t + \cdots + c_{n-s-1} t^{n-s-1} \in \mathbb{Z}[t]$$

such that $\Lambda = \mathscr{P}(S)$. Since the size of S is $(n-s) \times (n-s)$, we can choose the polynomial $\mathscr{P}(t)$ of degree less than or equal to $n-s-1$. Since the eigenvalues

of S are the primitive r-th root ζ_r of unity with $r \in R(n,s)$ by Lemma 2.2, the eigenvalues of Λ are $\mathscr{P}(\zeta_r)$. Furthermore, it is easy to find a corresponding eigenvector, since it coincides with an eigenvector v_r of S with eigenvalue ζ_r. In fact, the eigenvector v_r can be computed directly from (2.1) and we have

$$v_r = {}^{\mathrm{t}}(\zeta_r^{n-s-1}, \zeta_r^{n-s-2}, \dots, \zeta_r, 1). \tag{2.2}$$

Note that the constraint $-(1+\zeta_r^s+\cdots+\zeta_r^{s(d-2)}) = \zeta_r^{s(d-1)}$ from the first row of S holds because all $r \in R(n,s)$ divide n.

Proposition 2.3. *Let $\Lambda = \mathscr{P}(S) \in \mathbb{Z}[S]$ be an endomorphism of $\widehat{T}_s$. Assume that each ideal generated by $\mathscr{P}(\zeta_r)$ in $\mathbb{Z}[\zeta_r]$ $(r \in R(n,s))$ is prime to n. Then we have*

$$\operatorname{coker}\Lambda \cong \bigoplus_{r\in R(n,s)} \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)).$$

Proof. The proof is similar to that of [6, Proposition 2.2] (see the remark below) and involves diagonalizing Λ over the rings of cyclotomic integers.

For $r \in R(n,s)$, we define

$$f_r : \mathbb{Z}^{\oplus(n-s)} \longrightarrow \mathbb{Z}[\zeta_r] \quad \text{by} \quad (a_1, \cdots, a_{n-s}) \mapsto (a_1, \cdots, a_{n-s})v_r,$$

where v_r is the eigenvector given by (2.2). Since the eigenvalue of Λ corresponding to v_r is $\mathscr{P}(\zeta_r)$, we have the following commutative diagram of $\mathbb{Z}$-modules:

$$\begin{array}{ccc} \mathbb{Z}^{\oplus(n-s)} & \xrightarrow{\Lambda} & \mathbb{Z}^{\oplus(n-s)} \\ {\scriptstyle\oplus f_r}\downarrow & & \downarrow{\scriptstyle\oplus f_r} \\ \bigoplus_{r\in R(n,s)} \mathbb{Z}[\zeta_r] & \xrightarrow{\times\mathscr{P}(\zeta_r)} & \bigoplus_{r\in R(n,s)} \mathbb{Z}[\zeta_r] \end{array}.$$

From this diagram, we have an induced map

$$F : \operatorname{coker}\Lambda \longrightarrow \bigoplus_{r\in R(n,s)} \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r))$$

and the map makes the following diagram commutative and exact in rows:

$$\begin{array}{ccccc} \mathbb{Z}^{\oplus(n-s)} & \xrightarrow{\Lambda} & \mathbb{Z}^{\oplus(n-s)} & \longrightarrow & \operatorname{coker}\Lambda \\ {\scriptstyle\oplus f_i}\downarrow & & \downarrow{\scriptstyle\oplus f_i} & & \downarrow F \\ \bigoplus \mathbb{Z}[\zeta_r] & \xrightarrow{\times\mathscr{P}(\zeta_r)} & \bigoplus \mathbb{Z}[\zeta_r] & \longrightarrow & \bigoplus_{r\in R(n,s)} \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \end{array}.$$

If P is a diagonalizing matrix of Λ arising from eigenvectors v_r in (2.2), then we have

$$P^{-1}\Lambda P = \operatorname{diag}_{r\in R(n,s),\zeta_r\in U_r}(\mathscr{P}(\zeta_r)),$$

where U_r is the set of *all* r-th roots of unity. Therefore we have

$$\det \Lambda = \prod_{r \in R(n,s), \zeta_r \in U_r} \mathscr{P}(\zeta_r) = \prod_{r \in R(n,s)} N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}} \mathscr{P}(\zeta_r)$$

where $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}$ is the norm map from $\mathbb{Q}(\zeta_r)$ to $\mathbb{Q}$.

On the other hand, the determinant of P is a product of $\zeta_r - \zeta_{r'}$ $(r, r' \in R)$. Hence $\det P$ is a divisor of n. By our assumption, $\det \Lambda$ is prime to $\det P$. Hence the module sturucture is preserved by F. This completes the proof of the proposition. □

Remark 2.4. In the statement of [6, Proposition 2.2], the corresponding assumption $(\det \Lambda, n) = 1$ is needed.

The exsitence of cyclic self-isogeny on T_s follows from the following corollary.

Corollary 2.5. *Let m be an integer prime to n. An endomorphism $\Lambda = \mathscr{P}(S)$ of $\widehat{T}_s$ defines a cyclic self-isogeny of degree m on the algebraic torus T_s if and only if there exist a subset R of $R(n,s)$ and a set $\{m_r \mid r \in R\}$ of pairwise coprime integers whose product is m such that*

$$r \in R \Longrightarrow \mathbb{Z}[\zeta_r]/\mathscr{P}(\zeta_r) \cong \mathbb{Z}/m_r\mathbb{Z},$$
$$r \notin R \Longrightarrow \mathscr{P}(\zeta_r) \in (\mathbb{Z}[\zeta_r])^\times.$$

Proof. Let λ be a self-isogeny of T_s corresponding to Λ. The kernel of λ is isomorphic to cokernel of Λ. Hence the kernel is cyclic if and only if each factor has pairwise coprime order. This proves the corollary. □

Remark 2.6. In his article [8], especially in Section 2, Suwa showed the isomorphism

$$\widehat{T}_s \cong J_{G/H}, \tag{2.3}$$

where $J_{G/H}$ is defined as follows. Let $\nu_{G/H} : \mathbb{Z}[G/H] \longrightarrow \mathbb{Z}[G]$ be a left $\mathbb{Z}[G]$-module homomorphism given by $g \mapsto \sum_{h \in H} gh$. Then $J_{G/H}$ is defined as $\mathrm{Coker}(\nu_{G/H})$. He also pointed me out that the endomorphism ring of T_s can be deduced from (2.3) by standard calculation of $\mathbb{Z}[G]$-modules.

§3. Proof of the main theorem

In this section, we shall give a proof of the main theorem (Theorem 1.1). We use the notation in the statement of the theorem. Hence $K = k(\zeta_m)$ and M is an intermediate field such that $[M : k] = s$.

If $\mathscr{P}(t) \in \mathbb{Z}[t]$ is a polynomial of degree less than or equal to $n-s-1$ and S is the matrix defined by (2.1), then $\Lambda = \mathscr{P}(S)$ defines an endomorphism of the character module of the algebraic torus $T_s = \ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m)$ by Proposition 2.1. By Corollary 2.5, the endomorphism Λ corresponds to a cyclic isogeny λ from T_s to itself of degree m. The isogeny λ is defined over k, because Λ is compatible with the Galois action (see [7, Proposition 1.2.3]). If we write $\Lambda = (\alpha_{ij})$, then the isogeny λ is defined by

$$(X_1, X_2, \ldots, X_{n-s}) \mapsto \left(\prod_{j=1}^{n-s} X_j^{\alpha_{j1}}, \ldots, \prod_{j=1}^{n-s} X_j^{\alpha_{j,n-s}} \right) \tag{3.1}$$

on the split torus $\mathbb{G}_{m,K}^{n-s}$ of T_s.

Now we have a cyclic isogeny λ on T_s. If we can show that λ satisfies (1.2) and (1.3), then the Kummer duality (1.10) for T_s holds as we explained in Section 1. We first consider (1.2). Namely we shall show that every point in $\ker(\lambda)(\overline{k})$ is defined over k. Recall that the matrix $\Lambda = \mathscr{P}(S)$ has an eigenvalue $\mathscr{P}(\zeta_r)$ with $r \in R(n,s)$ and the corresponding eigenvector v_r is given by (2.2):

$$\Lambda v_r = \mathscr{P}(\zeta_r) v_r. \tag{3.2}$$

We may assume that $r \in R \subset R(n,s)$. Then reducing (3.2) modulo $\mathscr{P}(\zeta_r)$, we find $v_r \bmod \mathscr{P}(\zeta_r)$ is in the kernel of $\Lambda \bmod m_r$ under the isomorphism $\varphi_r : \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \cong \mathbb{Z}/m_r\mathbb{Z}$ of (1.7). Let $t_r = \varphi_r(\zeta_r)$. By our assumption $r \in R$, the additive group of the ring $\mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r))$ is cyclic. Since, in particular, m is prime to n, this implies that the principal ideal generated by $\mathscr{P}(\zeta_r)$ is a product of prime ideals of degree one with different residue characteristic (see [2, Theorem 4.2.10]). Therefore if p is a prime number dividing m_r, then we have $p \equiv 1 \pmod{r}$ for all $r \in R$ by the assumption $(m,n) = 1$. Moreover, the order of t_r modulo m_r is r. By Chinese remainder theorem, we can find an integer t satisfying $t \equiv t_r \pmod{m_r}$ for all $r \in R$. The order of $t \bmod m$ is $n = \operatorname{lcm}_{r\in R} r$. As a result, we see

$$\Lambda \begin{pmatrix} t^{n-s-1} \\ \vdots \\ t \\ 1 \end{pmatrix} \equiv \mathbf{0} \pmod{m}.$$

Simple calculation yields

$${}^{\mathrm{t}}S w_r = \zeta_r w_r,$$

where the eigenvector $w_r = ({w_r}^{(i)})$ is given by

$${w_r}^{(i)} = -\zeta_r^{d+1} \sum_{j=0}^{c} \zeta_r^{sj}, \quad \text{where } i - 1 = sc + d,\ 0 \le d < s.$$

Note that ${w_r}^{(n-s)} = 1$. By similar calculation as for Λ, we can show ${}^t\Lambda w \equiv 0 \pmod{m}$ with

$$w = \left(-t^{d+1} \sum_{j=0}^{c} t^{sj} \right)_{1 \leq i \leq n-s}. \tag{3.3}$$

Let us write $w = (w_i)_{1 \leq i \leq n-s}$. Since the degree of λ is m, it follows from (3.1) that $Z = (\zeta_m^{w_i})_{1 \leq i \leq n-s} \in \mathbb{G}_{m,K}^{n-s} \cong T_s \times_k K$ is contained in the kernel of λ. To prove $Z \in T_s(k)$, we use [7, Proposition 1.2.2]. It claims that $Z \in T_s(K)$ is k-rational if and only if the map $\widehat{T_s} \longrightarrow K^\times$ defined by $y \mapsto y(Z)$ is a G-module homomorphism. By the assumption (1.9), the inverse image σ_t of t generates the Galois group $G = \mathrm{Gal}(K/k)$ of order $n = \mathrm{lcm}_{r \in R} r$. Therefore the claim of the proposition is equivalent to

$$(Sy)(w) = \sigma_t(y(w)) \quad \text{for all } y \in \widehat{T_s}. \tag{3.4}$$

By linearity, it is enough to show (3.4) when y is a standard basis vector e_j $(1 \leq j \leq n-s)$. We compute

$$\text{the left hand side of (3.4)} = \begin{cases} w_{j+1} & \text{if } j \not\equiv 0 \pmod{s} \\ -w_1 + w_{j+1} & \text{if } j \equiv 0 \pmod{s} \end{cases}$$

and

$$\text{the right hand side of (3.4)} = t w_j.$$

The verification of these formulas is easy if we use (3.3). Thus we conclude $\ker \lambda(\overline{k}) = \ker \lambda(k)$.

We next show a weak version of Hilbert's theorem 90 (1.3). Taking Galois cohomology of the exact sequence

$$1 \longrightarrow \ker \lambda \longrightarrow T_s \xrightarrow{\lambda} T_s \longrightarrow 1,$$

we obtain

$$T_s(k) \xrightarrow{\lambda} T_s(k) \longrightarrow \mathrm{H}^1(k, \ker \lambda) \longrightarrow \ker \left(\lambda : \mathrm{H}^1(k, T_s) \longrightarrow \mathrm{H}^1(k, T_s) \right).$$

On the other hand, the exact sequence

$$1 \longrightarrow T_s \longrightarrow R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/M}} R_{M/k}\mathbb{G}_m \longrightarrow 1$$

yields the exact sequence

$$R_{K/k}\mathbb{G}_m(k) \xrightarrow{N_{K/M}} R_{M/k}\mathbb{G}_m(k) \longrightarrow \mathrm{H}^1(k, T_s) \longrightarrow \mathrm{H}^1(k, R_{K/k}\mathbb{G}_m).$$

By Shapiro's lemma and Hilbert's theorem 90, we have

$$\mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) \cong \mathrm{H}^1(K, \mathbb{G}_{m,K}) = 1.$$

Therefore under the natural isomorphism $R_{K/k}\mathbb{G}_m(k) \cong K^\times$, we obtain

$$\mathrm{H}^1(k, T_s) \cong M^\times / N_{K/M} K^\times.$$

Since $m = \deg \lambda$ is prime to n, it is also prime to $s = [K : M]$. Thus we obtain $\ker\big(\lambda : \mathrm{H}^1(k, T_s) \longrightarrow \mathrm{H}^1(k, T_s)\big) = 1$. Thus we have proved (1.3) for T_s.

Combining all these, we have a Kummer duality

$$T_s(k)/\lambda T_s(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker \lambda(\bar{k})).$$

This completes the proof of the main theorem.

Remark 3.1. A scheme-theoretic description of the kernel of λ is given in [8, Remark 3.5].

§4. Examples

In this section, we shall use Theorem 1.1 to construct all cyclic extensions of degree m over certain proper subfields of the m-th cyclotomic field $K = \mathbb{Q}(\zeta_m)$. The base field k will be taken such that K/k is a cyclic extension of degree n and M is an intermediate field of K/k satisfying $s = [M : k]$.

Example 4.1. Our first example is a simplest case where $n = 4$ and $s = 2$. We have $R(4, 2) = \{4\}$. We want to find a linear polynomial $\mathscr{P}(t)$ such that

$$\varphi_4 : \ \mathbb{Z}[\zeta_4]/(\mathscr{P}(\zeta_4)) \cong \mathbb{Z}/m\mathbb{Z} \tag{4.1}$$

for some integer m. We may assume $m > 2$. If m is of the from $p_0 p_1 \cdots p_r$ where $p_0 = 1$ or 2 and p_i $(r \geq i \geq 1)$ are distinct odd primes congruent to 1 modulo 4, then we can find $\mathscr{P}(t)$ satisfying (4.1), since $\mathbb{Z}[\zeta_4]$ is a unique factorization domain. Once we find such $\mathscr{P}(t)$ and m, we can choose the base field k as a fixed subfield of the group generated by $\varphi_4(\zeta_4)$ in $K = \mathbb{Q}(\zeta_m)$ under the natural isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Then we obtain an isomorphism corresponding to ν_k in (1.9).

Explicit examples of $\mathscr{P}(t)$ with small coefficients are given in the following table:

$\mathscr{P}(t)$	m	$\varphi_4(\zeta_4)$	$k = \mathbb{Q}(\zeta_m)^{\langle\varphi_4(\zeta_4)\rangle}$	$\mathrm{Irr}(\alpha_i, \mathbb{Q}, x)$
$2t+1$	5	2	$\mathbb{Q}$	
$3t+2$	13	8	$\mathbb{Q}(\alpha_1)$	$x^3 - x^2 - 4x - 1$
$4t+1$	17	4	$\mathbb{Q}(\alpha_2)$	$x^4 - x^3 - 6x^2 + x + 1$

Now let M be an intermediate field of K/k fixed by $\varphi_4(\zeta_4)^2$. In our case, we always have $\varphi_4(\zeta_4)^2 = -1$, since m is a square-free integer. Therefore our field M is the maximal real subfield of $\mathbb{Q}(\zeta_m)$.

The Kummer duality of the 2-dimensional torus

$$T_2 = \ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m)$$

implies that every cyclic extension of k of degree m is of the form $k(\lambda^{-1}(P))$, where $P \in T_2(k)$ and λ is a self-isogeny of T_2 corresponding to the character module homomorphism $\mathscr{P}(S)$, where $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ in this case. Since all 2-dimensional algebraic tori are rational varieties (see [9]), we can find a rational parameterization of $T_2(k)$. Fixing an isomorphism $T_2(k)$ into K, let $a\zeta_m + b{\zeta_m}^{-1} \in T_2(k)$ $(a, b \in M)$. Then $N_{K/M}(a\zeta_m + b{\zeta_m}^{-1}) = 1$ defines a conic and has a rational point $(a, b) = (1, 0)$. Using this point, we obtain a parameterization

$$(a,b) = \left(\frac{u^2 - v^2}{u^2 + ({\zeta_m}^2 + {\zeta_m}^{-2})uv + v^2}, \frac{2uv + ({\zeta_m}^2 + {\zeta_m}^{-2})v^2}{u^2 + ({\zeta_m}^2 + {\zeta_m}^{-2})uv + v^2} \right) \tag{4.2}$$

with $u, v \in k$.

Example 4.2. We study the case $m = 5$ in the previous example more closely. We write ζ for ζ_5 for simplicity. Let σ be the element of $\mathrm{Gal}(K/k)$ corresponding to $\varphi_4(\zeta_4) = 2$. Namely we have $\zeta^\sigma = \zeta^2$. On the split torus $\mathbb{G}_{m,K}^2$ of T_2, the matrix $\mathscr{P}(S) = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$ defines an endomorphism $(X_1, X_2) \mapsto (X_1{X_2}^2, {X_1}^{-2}X_2)$. If $P \in T_2(\mathbb{Q})$ corresponds to $\alpha \in K$ satisfying $N_{K/M}\alpha = 1$, then $L = \mathbb{Q}(\lambda^{-1}(P))$ is characterized as a unique quintic subfield over $\mathbb{Q}$ inside $\mathbb{Q}(\zeta_5, \sqrt[5]{\alpha^2\alpha^\sigma})$. A defining polynomial of L over $\mathbb{Q}$ with simple Galois action can be computed by the method in [5, Section 5] using the relations

$$X_1X_3 = 1 \text{ and } X_2X_4 = 1.$$

More precisely, for $\alpha_1 = a\zeta + b\zeta^{-1}, \alpha_2 = \sigma(\alpha_1) = a^\sigma\zeta^2 + b^\sigma\zeta^{-2}$, a defining polynomial is

$$\begin{aligned} F(Y) =& Y^5 - Y^3 + \mathrm{Tr}(\xi_2\alpha_1)Y^2 + \left(\frac{2}{25} + \mathrm{Tr}(\xi_1\alpha_1\alpha_2) \right) Y \\ &+ \left(\mathrm{Tr}(\xi_{01}{\alpha_1}^2\alpha_2) + \mathrm{Tr}(\xi_{02}\alpha_2) \right), \end{aligned}$$

where Tr is the trace map from $K(\alpha_1, \alpha_2)$ to $k(\alpha_1, \alpha_2)$ and

$$\xi_2 = \frac{1}{25}(2\zeta - \zeta^2 - 2\zeta^4 + \zeta^3), \qquad \xi_1 = \frac{1}{25}(\zeta + \zeta^4),$$

$$\xi_{01} = \frac{1}{625}(\zeta - 2\zeta^2 - \zeta^4 + 2\zeta^3), \qquad \xi_{02} = \frac{1}{125}(\zeta^4 - \zeta).$$

This polynomial from the Kummer theory of T_2 is simpler than the polynomial in [5, Section 5] obtained from that of $R^{(1)}_{K/k}\mathbb{G}_m$. Substituting (4.2), we obtain a 2-parameter polynomial defining all cyclic quintic extensions over $\mathbb{Q}$:

$$\begin{aligned} Y^5 - Y^3 &+ \frac{-2u^4 + 5u^3v - 3u^2v^2 + uv^3 + v^4}{5(u^4 - u^3v + u^2v^2 - uv^3 + v^4)}Y^2 \\ &+ \frac{2u^3v - u^2v^2 - 2uv^3 + v^4}{5(u^4 - u^3v + u^2v^2 - uv^3 + v^4)}Y \\ &+ \frac{u^8 + u^7v - 18u^6v^2 + 13u^5v^3 + 30u^4v^4 - 44u^3v^5 + 6u^2v^6 + 17uv^7 - 7v^8}{125(u^4 - u^3v + u^2v^2 - uv^3 + v^4)^2}. \end{aligned}$$

As we note in Section 1, our dimension $2 = \dim T_2$ is the smallest dimension to parameterize all quintic cyclic extensions over $\mathbb{Q}$ (see [3]).

Example 4.3. We consider the case where $n = 6$. There are two choices of $s > 1$. If we choose a smaller s, then the degree of $\mathscr{P}(t)$ may be larger. Note, however, the degree of the base field over the prime field is unchanged whichever s we choose. Here we take $s = 3$ and we have $R(6, 3) = \{2, 6\}$. Let $R = \{6\}$. We find the following examples:

$\mathscr{P}(t)$	m	$\varphi_6(\zeta_6)$	k
$t + 2$	7	5	$\mathbb{Q}$
$t^2 - 2t - 2$	13	10	$\mathbb{Q}(\sqrt{13})$

In both case, we have $\mathscr{P}(\zeta_2) = 1$.

Example 4.4. We give an example using multiple moduli. In the case where $n = 6$ and $s = 1$, the torus is a norm torus T_1. We have $R(6, 1) = \{2, 3, 6\}$. For the quartic polynomial $\mathscr{P}(t) = t^4 + t^3 + 2t^2 + 3t + 2$, we take $R = \{3, 6\}$ and we evaluate

$$\mathscr{P}(-1) = 1, \quad \mathscr{P}(\zeta_3) = 2\zeta_3 + 1, \quad \mathscr{P}(\zeta_6) = 4\zeta_6 - 1.$$

Thus we obtain

$$\begin{aligned} \mathbb{Z}[\zeta_3]/(2\zeta_3 + 1) &\cong \mathbb{Z}/3\mathbb{Z}, & \zeta_3 &\mapsto 1, \\ \mathbb{Z}[\zeta_6]/(4\zeta_6 - 1) &\cong \mathbb{Z}/13\mathbb{Z}, & \zeta_6 &\mapsto 10. \end{aligned}$$

This polynomial satisfies the conditions of Theorem 1.1. Let k be the field fixed by $\zeta_{39} \mapsto {\zeta_{39}}^{10}$ in $\mathbb{Q}(\zeta_{39})$, which is explicitly defined by $x^4 + x^3 - 11x^2 + 9x + 3$. The isogeny on $T_1 = R^{(1)}_{\mathbb{Q}(\zeta_{39})/k}\mathbb{G}_m$ associated to $\mathscr{P}(t)$ gives all cyclic extensions of degree 39 over k.

We use a computer algebra system Magma [1] to compute the examples in this section.

Acknowledgments. I would like to give sincere thanks to Professor Noriyuki Suwa whose comments and suggestions simplified and clarified the contents of this paper.

This research is supported in part by Grant-in-Aid for Scientific Research (C) (No. 24540011), Ministry of Education, Science, Sports and Culture, Japan.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[2] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 2000.

[3] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002.

[4] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447.

[5] ———, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 102–113.

[6] ———, *Descent Kummer theory via Weil restriction of multiplicative groups*, J. Number Theory **130** (2010), no. 3, 639–659.

[7] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139.

[8] N. Suwa, *Kummer theories for algebraic tori and normal basis problem*, Tokyo J. Math. **39** (2017), no. 3, 827–862.

[9] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998.

Masanari Kida
Department of Mathematics, Tokyo University of Science
Kagurazaka 1-3, Shinjuku, Tokyo 162-0827, Japan
E-mail: kida@rs.tus.ac.jp