Descent Kummer theory via Weil restriction of multiplicative groups

Masanari Kida

Department of Mathematics, University of Electro-Communications, 1-5-1 Chofugaoka Chofu, Tokyo 182-8585, Japan

1. Main theorem

Let \( \mathbb{G}_{m,k} \) be the multiplicative group defined over a field \( k \) and \( m \) a positive integer prime to the characteristic of \( k \). The \( m \)-th power map \( [m] : x \mapsto x^m \) is a separable endomorphism of \( \mathbb{G}_{m,k} \). We have an exact sequence

\[
1 \longrightarrow \ker[m] \longrightarrow \mathbb{G}_{m,k} \overset{[m]}{\longrightarrow} \mathbb{G}_{m,k} \longrightarrow 1 \quad \text{(exact)}.
\]

If all the points in the group \( \ker[m] \) of \( m \)-th roots of unity are all \( k \)-rational, namely if \( k \) contains an \( m \)-th root of unity, then this exact sequence yields the classical Kummer duality

\[
k^\times / (k^\times)^m \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker[m]).
\]

since the first cohomology group \( H^1(k, \mathbb{G}_m) \) vanishes by Hilbert’s theorem 90. Here the right hand side is the group of continuous homomorphisms. The isomorphism is given by \( k^\times \ni a \mapsto \chi_a \) where \( \chi_a \)
is a character defined by \( \chi_a(\sigma) = b^{1-\sigma} \) for \( \sigma \in \text{Gal}(\bar{k}/k) \) with \( b \in \bar{k} \) satisfying \( b^m = a \). This expression provides a simple description of a cyclic extension of degree \( m \) over \( k \): it is of the form \( k(\sqrt[m]{a}) \) for some \( a \in k^\times \). Besides this handy description of cyclic extensions, the Kummer theory has many applications in various areas of algebra and number theory. Thus it is quite desirable to have an analogue of the Kummer theory for fields without roots of unity. The aim of this paper is to give such a theory using the Weil restriction of the multiplicative groups.

Throughout this paper, we will use the following notation. For a positive integer \( m \), we denote a primitive \( m \)-th root of unity by \( \zeta_m \). For the choice of \( \zeta_m \), we impose the condition \( \zeta_m^d = \zeta_n \) if \( m = nd \). We write \( \mu_m = \langle \zeta_m \rangle \) for the group of \( m \)-th roots of unity. Let \( \varphi(m) \) be the Euler function giving the order of \( (\mathbb{Z}/(m))^\times \).

Our main theorem is as follows.

**Theorem 1.1.** Let \( m \) be a positive integer greater than 1 and \( n \) a positive divisor of \( \varphi(m) \). Suppose that there exists an integer-coefficient polynomial

\[
\mathcal{P}(t) = c_1 t + c_2 t^2 + \cdots + c_n t^{n-1} \in \mathbb{Z}[t]
\]

of degree \( n - 1 \) such that there exists an isomorphism

\[
\mathbb{Z}[\zeta_n]/(\mathcal{P}(\zeta_n)) \cong \mathbb{Z}/(m)
\]

and that

\[
\mathcal{P}(\zeta_n^i) \in \mathbb{Z}[\zeta_n^i]^\times \text{ for all } i \text{ with } (n, i) > 1
\]

holds. Let \( k \) be a field of characteristic prime to \( m \) such that the ring isomorphism (1.2) induces a group isomorphism

\[
\nu_k : \text{Gal}(k(\zeta_m)/k) \to \langle \zeta_n \text{ mod } \mathcal{P}(\zeta_n) \rangle.
\]

Denote \( k(\zeta_m) \) by \( K \). Then there exists a cyclic self-isogeny \( \lambda \) of degree \( m \) on the Weil restriction \( R_{K/k}\mathbb{G}_m \) for which we have \( \ker \lambda \cong \mathbb{Z}/(m) \) with trivial Galois action and the exact sequence attached to the isogeny \( \lambda \)

\[
1 \to \ker \lambda \to R_{K/k}\mathbb{G}_m \overset{\lambda}{\to} R_{K/k}\mathbb{G}_m \to 1 \quad \text{(exact)}
\]

induces a Kummer duality

\[
\kappa_k : R_{K/k}\mathbb{G}_m(k)/\lambda R_{K/k}\mathbb{G}_m(k) \xrightarrow{\sim} \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker(\bar{k})).
\]

Some comments are in order.

As we expected, the base field \( k \) does not contain the group of \( m \)-th roots of unity if \( n > 1 \). On the other hand, if \( n = 1 \) and \( \mathcal{P}(t) = m \), then the classical Kummer theory follows from Theorem 1.1. Thus our theorem is a natural generalization of the classical theory.

In our previous paper [5], we proved a similar Kummer duality using the norm torus \( R_{K/k}\mathbb{G}_m^{(1)} \), which is, by definition, the kernel of the norm map from the Weil restriction to the multiplicative group. Though the statement of [5, Theorem 1.2] looks different from Theorem 1.1, the scopes of the theorems are almost the same. But the above Kummer theory has several advantages against the Kummer theory by norm tori. One of these advantages is the simplicity of the proof. The structure of the endomorphism ring of \( R_{K/k}\mathbb{G}_m \) is easier to grasp than that of \( R_{K/k}\mathbb{G}_m^{(1)} \) and the Galois cohomology is also simpler. These two points make the proof easier than the norm torus case. The simple structure of the endomorphism ring also enables us to find more explicit examples of fields admitting this type
of Kummer theory easier than before. Furthermore, we can show that the Kummer theory for $R_{K/k} \mathbb{G}_m$ always induces that for $R_{K/k}^{(1)} \mathbb{G}_m$ (Theorem 5.1). In the last section, we deduce an explicit relation between our Kummer theory and the classical one (Theorem 6.1 and Proposition 6.3). We cannot expect a similar theorem in the norm torus case because it does not contain the classical Kummer theory. Other comparisons of these two theories will be made in the following sections.

The rest of the paper is organized as follows. After some investigations on the endomorphisms of $R_{K/k} \mathbb{G}_m$ in the next section, we shall prove the main theorem in Section 3. In Section 4 we study conditions for fields to admit this Kummer theory. Some explicit examples will be given there. In the final section, we prove a theorem on base change.

2. The endomorphism ring of $R_{K/k} \mathbb{G}_m$

Let $K/k$ be a cyclic extension of degree $n$ with Galois group $G = \text{Gal}(K/k)$ generated by $\sigma$. In this section, we shall study the endomorphisms of $R_{K/k} \mathbb{G}_m$.

It is known that the character module $\hat{R}_{K/k} \mathbb{G}_m = \text{Hom}_{k\text{-schemes}}(R_{K/k} \mathbb{G}_m, \mathbb{G}_m, k)$ is isomorphic to $\mathbb{Z}[G]$ as $G$-modules. We compute the endomorphism ring of this Galois module.

**Proposition 2.1.** The endomorphism ring of the character module $\hat{R}_{K/k} \mathbb{G}_m$ is isomorphic to the ring of circulant matrices of order $n$:

$$C_n = \left\{ \text{circ}(c_1, c_2, \ldots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix} | c_1, c_2, \ldots, c_n \in \mathbb{Z} \right\}.$$

**Proof.** By taking a standard basis $1, \sigma, \ldots, \sigma^{n-1}$ of $\mathbb{Z}[G]$, the generator $\sigma$ acts by the matrix

$$\Sigma = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

Hence the matrices corresponding to the $G$-endomorphisms of the character module agree with the centralizer of $\Sigma$. Solving the linear system yields the result. \[ \square \]

For $\text{circ}(c_1, c_2, \ldots, c_n) \in C_n$, we associate a polynomial of degree $n-1$ defined by

$$\mathcal{P}(t) = c_1 + c_2 t + \cdots + c_n t^{n-1}$$

called the representer of the circulant matrix $\text{circ}(c_1, c_2, \ldots, c_n)$ (see [3, p. 68]. This textbook serves as a basic reference for circulant matrices). It is easy to see (or refer to [3, (3.2.3)]) that the eigenvalues of $\text{circ}(c_1, c_2, \ldots, c_n)$ are $\mathcal{P}(\zeta_d^i)$ ($i = 0, \ldots, n-1$).

**Proposition 2.2.** Let $\Lambda = \text{circ}(c_1, c_2, \ldots, c_n) \in C_n$. Define a linear transformation of $\mathbb{Z}^{\oplus n}$, also denoted by $\Lambda$, by the formula $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n) \Lambda$. Then we have

$$\text{coker} \Lambda \cong \bigoplus_{d|n} \mathbb{Z}[\zeta_d]/\left(\mathcal{P}(\zeta_d)\right)$$

where the direct sum is taken over all positive divisors of $n$. 

Proof. Let $\mathcal{P}(t)$ be the representer of $\Lambda$. For $i = 0, 1, \ldots, n - 1$, set $d_i = n/(n, i)$ and define

$$f_i : \mathbb{Z}^n \rightarrow \mathbb{Z}[\zeta_{d_i}] \quad \text{by} \quad (a_1, \ldots, a_n) \mapsto a_1 + a_2 \zeta_{d_i}^i + \cdots + a_n \zeta_{d_i}^{i(n-1)}.$$ 

Then a simple computation shows that the following diagram of $\mathbb{Z}$-modules commutes:

$$\begin{array}{ccc}
\mathbb{Z}^n & \xrightarrow{\Lambda} & \mathbb{Z}^n \\
\downarrow_{f_i} & & \downarrow_{f_i} \\
\mathbb{Z}[\zeta_{d_i}] & \xrightarrow{\times \mathcal{P}(\zeta_{d_i}^i)} & \mathbb{Z}[\zeta_{d_i}].
\end{array}$$

Gluing up for all $d_i$, we have a commutative diagram with exact rows

$$\begin{array}{cccc}
\mathbb{Z}^n & \xrightarrow{\Lambda} & \mathbb{Z}^n & \rightarrow \mathrm{coker} \Lambda & \rightarrow 0 \\
\oplus f_i & & \oplus f_i & & \\
\bigoplus_{d_i \mid n} \mathbb{Z}[\zeta_{d_i}] & \xrightarrow{\times \prod_{d_i \mid n} \mathcal{P}(\zeta_{d_i})} & \bigoplus_{d_i \mid n} \mathbb{Z}[\zeta_{d_i}] & \rightarrow \bigoplus_{d_i \mid n} \mathbb{Z}[\zeta_{d_i}] / (\mathcal{P}(\zeta_{d_i})) & \rightarrow 0.
\end{array}$$

A well-defined homomorphism

$$F : \mathrm{coker} \Lambda \rightarrow \bigoplus_{d_i \mid n} \mathbb{Z}[\zeta_{d_i}] / (\mathcal{P}(\zeta_{d_i}))$$

is induced and it makes the following diagram commutative and exact in rows:

$$\begin{array}{ccc}
\mathbb{Z}^n & \xrightarrow{\Lambda} & \mathbb{Z}^n \\
\downarrow_{\oplus f_i} & & \downarrow_{\oplus f_i} \\
\mathrm{Im}(\oplus f_i) & \xrightarrow{\Delta} & \mathrm{Im}(\oplus f_i) \\
\downarrow & & \downarrow \\
\mathrm{coker} \Lambda & \xrightarrow{F} & \mathrm{coker} \Lambda
\end{array}$$

where $\Delta$ is the multiplication-by-$\prod_{d_i \mid n} \mathcal{P}(\zeta_{d_i})$ map. It is easy to verify that $F$ is injective. Thus we have an injection

$$\mathrm{coker} \Lambda \hookrightarrow \bigoplus_{d_i \mid n} \mathbb{Z}[\zeta_{d_i}] / (\mathcal{P}(\zeta_{d_i})).$$

Now we compute the order of these two groups. For the group on the left hand side, we have

$$\# \mathrm{coker} \Lambda = \det \Lambda = \prod_{i=0}^{n-1} \mathcal{P}(\zeta_{n}^i) = \prod_{d_i \mid n} \prod_{i \mid n/d} \mathcal{P}(\zeta_{d_i}^i) = \prod_{d_i \mid n} N_{\mathbb{Q}(\mathcal{P}(\zeta_d))}/\mathbb{Q} \mathcal{P}(\zeta_{d_i}),$$

where $N_{\mathbb{Q}(\mathcal{P}(\zeta_d))}/\mathbb{Q}$ is the norm map from $\mathbb{Q}(\mathcal{P}(\zeta_d))$ to $\mathbb{Q}$. On the other hand, for the group on the right hand side, we readily obtain

...
\[
\# \bigoplus_{d|n} \mathbb{Z}[\zeta_d] / (\mathcal{P}(\zeta_d)) = \prod_{d|n} N_{\mathbb{Q}(\mathcal{P}(\zeta_d))/\mathbb{Q}}(\mathcal{P}(\zeta_d)).
\]

Therefore the injection in the above is, in fact, an isomorphism. This completes the proof of the proposition. □

3. The proof of the main theorem

In this section, we shall give the proof of the main theorem (Theorem 1.1). We use the notation in the statement of the theorem. In particular, let \( k \) be a field satisfying the assumptions of the theorem and set \( K = k(\zeta_n) \).

We start with some remarks. When \( \mathbb{Z}[\zeta_n] \neq \mathbb{Z} \), the additive group of the residue ring \( \mathbb{Z}[\zeta_n] / \mathcal{P}(\zeta) \) is cyclic if and only if the ideal generated by \( \mathcal{P}(\zeta) \) is a product of prime ideals of degree one with different residue characteristic (see [2, Theorem 4.2.10]). Therefore, in this case, \( m \) must be a square-free integer. By the decomposition law in the cyclotomic field \( \mathbb{Q}(\zeta_n) \), every prime factor of \( m \) is congruent to 1 modulo \( n \). In particular, \( m \) is prime to \( n \). It follows from this that the order of \( \zeta_n \) mod \( \mathcal{P}(\zeta_n) \) is \( n \). Hence the order of the Galois group \( G \) of \( \mathbb{Q}(\zeta_n) \) is also \( n \).

Now we consider the torus \( T = R_{K/k} \mathbb{G}_m \). Using the coefficients of \( \mathcal{P}(t) \in \mathbb{Z}[t] \) given in (11), we form a circulant matrix \( \Lambda = \text{circ}(c_1, c_2, \ldots, c_n) \in \mathbb{C}_n \). By Proposition 2.1, the matrix \( \Lambda \) defines a \( G \)-endomorphism of the character module \( \hat{T} \) and thus induces an isogeny on the split torus \( \mathbb{G}_{m,K}^n \) of \( T \) defined over \( K \) by

\[
(X_1, X_2, \ldots, X_n) \mapsto \left( \prod_{j=1}^n X_j^{c_j}, \prod_{j=1}^n X_j^{c_{j-1}}, \ldots, \prod_{j=1}^n X_j^{c_{n+1}} \right)
\]

with the cyclic notation \( c_i = c_i \mod n \). By Proposition 2.2 and the assumptions (1.2) and (1.3), \( \Lambda \) has a cyclic cokernel of order \( m \). Let \( \lambda \) be an endomorphism of the torus \( T \) induced from \( \Lambda \). By the duality of the categories (see [10, 1.3]), \( \lambda \) is an isogeny of degree \( m \). We shall show that every point in the ker \( \lambda(k) \) is a \( k \)-rational point. Since \( \Lambda = \text{circ}(c_1, c_2, \ldots, c_n) \) is diagonalized by the Fourier matrix (see [3, 3.2]), we have

\[
\Lambda \begin{bmatrix}
\zeta_n^0 \\
\zeta_n^1 \\
\zeta_n^2 \\
\vdots \\
\zeta_n^{n-1}
\end{bmatrix} = \mathcal{P}(\zeta_n) \begin{bmatrix}
\zeta_n^0 \\
\zeta_n^1 \\
\zeta_n^2 \\
\vdots \\
\zeta_n^{n-1}
\end{bmatrix}.
\]

Considering the both sides modulo \( \mathcal{P}(\zeta_n) \), we see that

\[
\{ \zeta_n^0 \mod \mathcal{P}(\zeta_n), \ldots, \zeta_n^{n-1} \mod \mathcal{P}(\zeta_n) \}
\]

is contained in the kernel of \( \Lambda \mod m \). Since the kernel of \( \lambda \) is killed by the \( m \)-th power map, this means that \( (\zeta, \zeta^s, \ldots, \zeta^{s^{n-1}}) \in \mathbb{C}_{m,K}^n \) is contained in the kernel of \( \lambda \) (see (3.1)), where \( s \) is an element of \( \mathbb{Z}/(m)^X \) corresponding to \( \zeta_n \) mod \( \mathcal{P}(\zeta_n) \) by (1.3). Since the order of this element is \( m \), the group ker \( \lambda(k) \) coincides with the group generated by \( s \). Since \( s \) is also a generator of \( G \) by the isomorphism \( \psi_k \) in (1.4), this group agrees with the subgroup of the \( m \)-th roots of unity isomorphically contained in \( T(k) \cong K^X \). We conclude that \( \lambda \) is a cyclic endomorphism of \( T \) satisfying ker \( \lambda(k) \subset T(k) \). Therefore we have an exact sequence:

\[
1 \longrightarrow \ker \lambda \longrightarrow T \overset{\lambda}{\longrightarrow} T \longrightarrow 1 \quad (\text{exact}).
\]
Taking Galois cohomology, we obtain the following exact sequence:

$$T(k) \xrightarrow{\lambda} T(k) \longrightarrow H^1(k, \ker \lambda) \longrightarrow \ker(\lambda : H^1(k, T) \longrightarrow H^1(k, T)).$$

Here we abbreviate $H^1(\text{Gal}(\overline{k}/k), V(\overline{k}))$ as $H^1(k, V)$ for any algebraic group $V$. By Shapiro’s lemma and Hilbert’s theorem 90, we have

$$H^1(k, T) \cong H^1(K, \mathbb{G}_m) = \{1\}.$$ 

Also since $\text{Gal}(\overline{k}/k)$ acts trivially on $\ker \lambda$, we see

$$H^1(k, \ker \lambda) = \text{Hom}_{\text{cont}}(\text{Gal}(\overline{k}/k), \ker \lambda(\overline{k})).$$

Combining all these, we have a Kummer duality

$$\kappa_k : T(k)/\lambda T(k) \xrightarrow{\lambda} \text{Hom}_{\text{cont}}(\text{Gal}(\overline{k}/k), \ker \lambda(\overline{k})).$$

This completes the proof of Theorem 1.1.

**Remark 3.1.** Here we make some comments on a possible generalization of our main result in the category of $k$-tori.

Let $T_1$ and $T_2$ be algebraic tori defined over $k$. First we assume that there exists an isogeny $\lambda/k : T_1 \longrightarrow T_2$. (3.2)

Then from the exact sequence

$$1 \longrightarrow \ker(\lambda) \longrightarrow T_1 \xrightarrow{\lambda} T_2 \longrightarrow 1,$$

we have an exact sequence

$$1 \longrightarrow T_2(k)/\lambda T_1(k) \longrightarrow H^1(k, \ker(\lambda)(\overline{k})) \longrightarrow H^1(k, G(\overline{k}))[\lambda].$$

Suppose that $\lambda$ satisfies

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

and that we have

$$\text{a weak Hilbert’s theorem 90: } H^1(k, T_1(\overline{k}))[\lambda] = 1,$$ (3.4)

then we can obtain a Kummer duality:

$$T_2(k)/\lambda T_1(k) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\overline{k}/k), \ker(\lambda)(\overline{k})).$$ (3.5)

The first two conditions (3.2) and (3.3) will probably lead to certain arithmetic and Diophantine conditions as our case and this part seems to be the most difficult part for the generalization. It is known that the property (3.4) holds for quasi-trivial tori. Although (3.2), (3.3) and (3.4) imply the Kummer duality (3.5), it would be useful only if we could control the $k$-rational points $T_2(k)$. This is possible, for example, if the variety $T_2$ is $k$-birational to an affine space over $k$. There are many
research on this rationality problem by Swan [11], Voskresenskiĭ [12], Lenstra [8] and others. See [13, Chapter 3] for the detail and further references.

The author would like to thank the referee for kind comments on this remark.

4. Fields admitting Kummer theory

By Theorem 1.1, we can descend the field of definition of the classical Kummer duality. For this reason we may call this theory a descent Kummer theory. In this section, we investigate which fields admit this descent Kummer theory. For the case of norm tori, we consider this problem in [5, Section 5] and [6, Section 3]. As a result, Theorem 1.1 can be applied to as much fields as the norm torus case.

Proposition 4.1. Let \( m \) be a square-free positive integer and \( n \) a prime divisor of \( \varphi(m) \). Suppose that there exists an algebraic integer \( \lambda \in \mathbb{Z}[\zeta_n] \) with \( |N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)^\lambda| = m \). Then we can find a polynomial \( \mathcal{P}(t) \in \mathbb{Z}[t] \) of degree \( n - 1 \) satisfying the assumptions of Theorem 1.1. In particular, the Kummer duality holds in this case.

Proof. For simplicity, we write \( \zeta \) for \( \zeta_n \) in this proof.

Let \( g \) be a primitive root modulo \( n \). We consider a cyclotomic unit \( \eta = \zeta^g - 1 = 1 + \zeta + \cdots + \zeta^{g-1} \in \mathbb{Z}[\zeta] \) (see [14, Lemma 1.3]). Since \( \eta \equiv g \pmod{(1 - \zeta)} \) and \( \lambda \not\equiv 0 \pmod{(1 - \zeta)} \), there exists an integer \( i \) such that

\[
\lambda \eta^i \equiv \pm 1 \pmod{(1 - \zeta)}.
\]

We will choose a correct sign later. Set \( \lambda' = \lambda \eta^i \). If we can solve the Diophantine equation

\[
\begin{align*}
  c_1 + c_2 \zeta + \cdots + c_n \zeta^{n-1} &= \lambda', \\
  c_1 + c_2 + \cdots + c_n &= \pm 1,
\end{align*}
\]

(4.1)

then \( \mathcal{P}(T) = c_1 + c_2 T + \cdots + c_n T^{n-1} \) obviously satisfies the assumptions of the theorem. In the first equation of (4.1), we have

\[
(c_1 - c_n) + (c_2 - c_n) \zeta + \cdots + (c_{n-1} - c_n) \zeta^{n-2} = \lambda'.
\]

Since \( 1, \zeta, \ldots, \zeta^{n-2} \) are linearly independent (recall that \( n \) is a prime), \( a_i = c_i - c_n \) \((i = 1, \ldots, n - 1)\) are uniquely determined by \( \lambda' \). Substituting these quantities to the second equation of (4.1), we obtain

\[
a_1 + \cdots + a_{n-1} + nc_n = \pm 1.
\]

(4.2)

We have to prove the existence of \( c_n \) satisfying this equation. From the assumption on \( \lambda' \), it follows that

\[
a_1 + a_2 + \cdots + a_{n-1} + a_n \equiv a_1 + a_2 \zeta + \cdots + a_{n-1} \zeta^{n-2} = \lambda' \equiv \pm 1 \pmod{(1 - \zeta)}.
\]

From \( \mathbb{Z}[\zeta]/(1 - \zeta) \cong \mathbb{Z}/(n) \), it follows that \( a_1 + \cdots + a_{n-1} \equiv \pm 1 \pmod{n} \). Hence by choosing an appropriate sign in (4.2), we can find an integer \( c_n \). This proves the proposition. \( \square \)

If \( \mathbb{Z}[\zeta_n] \) is a principal ideal domain, there always exists an algebraic integer \( \lambda \) with norm \( \pm m \) in this ring (see the remarks in the beginning of Section 3). There are 29 such \( n > 1 \) (see [14, Chapter 11]).
We give some examples of $\mathcal{P}(t)$ for small $n$. In the following examples, we assume that the characteristic of $k$ is zero.

**Example 4.2.** We consider the case where $n = 2$. Let $m$ be an odd square-free integer. Then

$$\mathcal{P}(t) = \frac{m+1}{2} + \frac{1-m}{2}t$$

satisfies $\mathcal{P}(1) = 1$ and $\mathcal{P}(-1) = m$. Therefore the determinant of the circulant matrix corresponding to $\mathcal{P}(t)$ is $m$ and the isogeny of $T$ determined by the circulant satisfies the conditions of Theorem 1.1. Let $K = \mathbb{Q}(\zeta_m)$ and define $k = \mathbb{Q}(\zeta_m)^{(-1 \mod \mathcal{P}(-1))}$. The field $k$ is the maximal real subfield of $K$. Thus we have $[K:k] = 2$. Let $T = K^{\mathcal{P}} \mathbb{G}_m$ be a 2-dimensional torus. The circulant matrix associated to $\mathcal{P}(t)$ induces the endomorphism of the split torus of $T$:

$$\overline{\lambda} : \mathbb{G}_m^2 \to \mathbb{G}_m^2, \quad (X_1, X_2) \mapsto \left( X_1^{\frac{m+1}{2}}, X_2^{\frac{1-m}{2}}, X_1^{\frac{1-m}{2}}, X_2^{\frac{m+1}{2}} \right).$$

We have $\ker \overline{\lambda}(K) = \langle (\zeta_m, \zeta_m^{-1}) \rangle$. The isogeny $\lambda$ on $T$ induces a quadratic descent Kummer theory:

$$\kappa_k : T(k)/\lambda T(k) \xrightarrow{\sim} \text{Hom}_\text{cont}(\text{Gal}(\bar{k}/k) \ker \lambda(\bar{k})).$$

It is possible to compute a cyclic polynomial defining this Kummer extension by the method developed in [5, Section 6] and [6]. Here we only give a result for the case $m = 3$ without mentioning to the detail. In this case the base field $k$ is the field of rational numbers. A cyclic cubic polynomial parametrized by $v_1 + \sqrt{-3}v_2 \in \mathbb{Q}$ is

$$X^3 - \frac{3}{4}(v_1^2 + 3v_2^2)X - \frac{1}{4}(v_1^2 + 3v_1v_2^2).$$

The discriminant of the polynomial is $(\frac{9v_2^2}{4})(v_1^2 + 3v_2^2)^2$. In this way, we obtain a rational parametrization of the cyclic cubic fields over $\mathbb{Q}$, whereas, if we use a norm torus $K^{(1)}_{k/\mathbb{Q}} \mathbb{G}_m$, we have a projective parametrization (see [5, Example 6.1]). This is one of the advantages of using $K^{(1)}_{k/\mathbb{Q}} \mathbb{G}_m$.

On the other hand, if we take

$$\mathcal{P}(t) = \frac{m+1}{2} + \frac{m-1}{2}t,$$

then the determinant of the corresponding circulant matrix $\text{circ}(\frac{m+1}{2}, \frac{m-1}{2})$ is also $m$. Although the matrix commutes with $\Sigma$ and does define a $G$-module endomorphism of $\overline{T}$, this $\mathcal{P}(t)$ does not satisfy the assumption of the theorem: $\mathcal{P}(1) = m$ and $\mathcal{P}(-1) = 1$. We can show that the kernel of the corresponding endomorphism on $T$ does not consist of $k$-rational points.

**Example 4.3.** In this example, we consider a composite case $n = 4$. Let $m$ be a prime number congruent to 1 modulo 4. As in the norm torus case [6, Lemma 1], it is always possible to find an endomorphism $\lambda$ of degree $m$ inducing a quartic descent Kummer theory. Let $a$ and $b$ be integers satisfying $m = a^2 + b^2$. Such integers always exist by the condition on $m$. It is easy to see that $a$ and $b$ have different parities. Hence we may assume that $a$ is even. Let

$$\mathcal{P}(t) = \frac{a}{2} + \frac{b+1}{2}t - \frac{a}{2}t^2 + \frac{1-b}{2}t^3.$$

Then we have $\mathcal{P}(1) = 1$, $\mathcal{P}(-1) = -1$, $\mathcal{P}(\sqrt{-1}) = a + b\sqrt{-1}$ as required.
Example 4.4. Here is another composite example $n = 6$. Let $m$ be a square-free positive integer such that $6|\varphi(m)$. Let $\zeta = \zeta_6$. We have to find a polynomial $P(t)$ of degree 5 such that the absolute value of the norm of $P(\zeta)$ is $m$ and $P(\zeta^2) \in \mu_6$, $P(\zeta^3) \in \mu_2$ and $P(1) \in \mu_2$. Since $\mathbb{Z}[\zeta]$ is a principal ideal domain, we can find $\xi = a + b\zeta \in \mathbb{Z}[\zeta]$ such that

$$|N_{Q(\zeta)/Q}(\xi)| = |a^2 + ab + b^2| = m.$$ 

The orbit of $a + b\zeta$ under the multiplication of the elements in $\mu_6 = (\mathbb{Z}[\zeta])^\times$ consists of

- $a + b\zeta, \quad -b + (a + b)\zeta, \quad (-a - b) + a\zeta, \quad a - b\zeta, \quad b - (a + b)\zeta, \quad (a + b) - a\zeta.$

Since $|a^2 + ab + b^2| = m \equiv 1 \pmod{6}$, we may assume that $(a \pmod{6}, b \pmod{6})$ is either $(1, 0), (1, 2)$ or $(1, 3)$. If $a \equiv 1, b \equiv 0 \pmod{6}$, let

$$P(t) = \frac{1}{6} \left((2a + b - 4) + (a + 2b - 1)t + (-a + b + 1)t^2 \right.$$

$$\left. + (-a - 2b + 1)t^3 + (a - b + 1)t^4 + (a - b - 1)t^5\right).$$

Then we have

$$P(\zeta) = a + b\zeta, \quad P(\zeta^2) = P(\zeta^3) = P(1) = 1.$$ 

Similarly we have, for $a \equiv 1, b \equiv 2 \pmod{6},$

$$P(t) = \frac{1}{6} \left((2a + b - 4) + (a + 2b + 1)t + (-a + b - 1)t^2 \right.$$

$$\left. + (-a - 2b - 1)t^3 + (a - b - 1)t^4 + (a - b + 1)t^5\right),$$

$$P(\zeta) = a + b\zeta, \quad P(\zeta^2) = P(1) = 1, \quad P(\zeta^3) = -1.$$ 

and, for $a \equiv 1, b \equiv 3 \pmod{6},$

$$P(t) = \frac{1}{6} \left((2a + b + 1) + (a + 2b - 1)t + (-a + b + 4)t^2 \right.$$

$$\left. + (-a - 2b + 1)t^3 + (a - b + 2)t^4 + (a - b + 2)t^5\right),$$

$$P(\zeta) = a + b\zeta, \quad P(\zeta^2) = P(1) = 1, \quad P(\zeta^3) = -1.$$ 

In any case a required polynomial exists.

Since this sextic descent has not been found in the norm torus case, we study this case more closely for a specific example $m = 7$. We have $7\mathbb{Z}[\zeta] = (1 + 2\zeta)(3 - 2\zeta)$. For $\zeta = 1 + 2\zeta$, we can take $P(t) = t - t^3 - t^4$. For $\zeta = 3 - 2\zeta$, we have $\zeta^3 = 1 - 3\zeta$. For this element, we can take $P(t) = -t + t^4 - t^5$. In both cases, $\zeta \pmod{7}$ fixes $P(\zeta)$ generates the full Galois group $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Therefore, the isogeny $\lambda$ of $R_{Q(\zeta)/\mathbb{Q}} \cup \mathbb{G}_m$ defined by either of $P(t)$ induces a Kummer duality over $\mathbb{Q}$:

$$\kappa_{Q} : R_{Q(\zeta)/\mathbb{Q}} \cup \mathbb{G}_m(\mathbb{Q}) \to \text{Hom}_{\text{cont}}(\text{Gal}(\mathbb{Q}/\mathbb{Q}) \text{ker } \lambda(\mathbb{Q})).$$

Since we do not use $\zeta_6$ in this example any more, we change the notation and denote $\zeta_7$ by $\zeta$. We take a normal basis $\zeta, \zeta^3, \zeta^5, \zeta^6, \zeta^4\zeta^5$ of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Let $P = (u_1, u_2, u_3, u_4, u_5, u_6)$ be a rational point in $R_{Q(\zeta)/\mathbb{Q}} \cup \mathbb{G}_m(\mathbb{Q})$ whose coordinates are taken with respect to the above normal basis.
Also by this normal basis, we can determine an isomorphism $\phi$ from $R_{Q(\zeta)/Q}G_m$ to $G_m^{6, Q(\zeta)}$ and let $\phi(P) = (\alpha_1, \ldots, \alpha_6)$. Hence we have

$$\alpha_i = u_1(\zeta)^{\tau^{-1}} + u_2(\zeta^3)^{\tau^{-1}} + u_3(\zeta^2)^{\tau^{-1}} + u_4(\zeta^6)^{\tau^{-1}} + u_5(\zeta^4)^{\tau^{-1}} + u_6(\zeta^5)^{\tau^{-1}}, \quad (i = 1, \ldots, 6)$$

where $\tau : \zeta \mapsto \zeta^3$ is a generator of $\text{Gal}(Q(\zeta)/Q)$. We take a point $Q = (x_1, \ldots, x_6) \in R_{Q(\zeta)/Q}G_m(\bar{Q})$ such that $\lambda(Q) = P$. Then we can easily verify that a generator of Galois group of the Kummer extension $Q(\zeta)/Q$ acts as

$$x_1 \mapsto -x_4 \mapsto x_4 - x_6 \mapsto x_6 - x_5 \mapsto x_5 - x_2 \mapsto x_2 - x_3 \mapsto x_3 - x_1 \mapsto x_1.$$

This shows that every cyclic extension of $Q$ of degree 7 is of the form $Q(x_1)$ with some $P \in R_{Q(\zeta)/Q}G_m(\bar{Q})$. We can compute the minimal polynomial $F(X)$ of $x_1$ by computing

$$F(X) = (X - x_1)(X + x_4)(X - x_4 + x_6)(X - x_6 + x_5)(X - x_5 + x_2)(X - x_2 + x_3)(X - x_3 + x_1).$$

Actually, we have, for $\mathcal{P}(t) = t - t^3 - t^4$,

$$F(X) = F(u_1, u_2, u_3, u_4, u_5, u_6; X)$$

$$= X^7 + \frac{1}{N} \text{Tr}\left( \frac{1}{14} (\zeta^5 + \zeta^2 - 2) \alpha_1 \alpha_2 \alpha_4 \alpha_5 \right) X^5$$

$$+ \frac{1}{49N} \text{Tr}\left( -2\zeta^5 - \zeta^4 + \zeta^3 + 2\zeta^2 \right) \alpha_1 \alpha_2 \alpha_4 + \frac{1}{3} \left( -4\zeta^4 - 4\zeta^2 - 4\zeta - 2 \right) \alpha_1 \alpha_3 \alpha_5 \right) X^4$$

$$+ \frac{1}{343N^2} \text{Tr}\left( -6\zeta^5 - 2\zeta^4 - 2\zeta^3 - 6\zeta^2 - 5 \right) \alpha_2 \alpha_3 \alpha_4 \alpha_5 \alpha_6^2$$

$$+ (-8\zeta^5 + 2\zeta^4 + 2\zeta^3 - 8\zeta^2 + 12) \alpha_1^2 \alpha_2^2 \alpha_4^2 \alpha_5^2$$

$$+ \frac{1}{2} \left( 9\zeta^5 + 3\zeta^4 + 3\zeta^3 + 9\zeta^2 - 3 \right) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4 \alpha_5 \alpha_6$$

$$+ \frac{1}{2} \left( -3\zeta^5 + 6\zeta^4 + 6\zeta^3 - 3\zeta^2 - 6 \right) \alpha_1^2 \alpha_2 \alpha_3^2 \alpha_4 \alpha_5 \alpha_6$$

$$+ \frac{1}{2} \left( -2\zeta^5 - 3\zeta^4 - 3\zeta^3 - 2\zeta^2 + 3 \right) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4^2 \alpha_5 \alpha_6 \right) X^3$$

$$+ \frac{1}{2401N^2} \text{Tr}\left( (\zeta^5 + 2\zeta^4 + 10\zeta^3 + 11\zeta^2 + 12\zeta + 6) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4 \right) X^2$$

$$+ (-4\zeta^5 - 8\zeta^4 - 12\zeta^3 - 18\zeta^2 - 20\zeta - 10) \alpha_1^3 \alpha_3 \alpha_4 \alpha_5^2$$

$$+ (-18\zeta^5 + 13\zeta^4 - 9\zeta^3 - 12\zeta^2 + 6\zeta + 3) \alpha_1^2 \alpha_2^2 \alpha_4^2 \alpha_5$$

$$+ (3\zeta^5 - 4\zeta^4 - 5\zeta^3 - 9\zeta^2 - 6\zeta - 3) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4^2 \alpha_6$$

$$+ (6\zeta^5 + 12\zeta^4 + 4\zeta^3 + 10\zeta^2 + 16\zeta + 8) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4 \alpha_5 \alpha_6$$

$$+ (-5\zeta^5 - 10\zeta^4 + 20\zeta^3 + 15\zeta^2 + 10\zeta + 5) \alpha_1^2 \alpha_2 \alpha_3 \alpha_4 \alpha_5 \alpha_6 \right) X.$$
\[\begin{align*}
&+ \frac{1}{2401N^3} \text{Tr}((3\zeta^5 + 6\zeta^4 + 6\zeta^3 + 3\zeta^2)\alpha_1^4\alpha_2\alpha_3^2\alpha_4^2\alpha_6^2 \\
&+ (-2\zeta^4 - 2\zeta^3 - 1)\alpha_1^4\alpha_2\alpha_3^2\alpha_4^2\alpha_6^2 + (-4\zeta^5 - 6\zeta^4 - 6\zeta^3 - 4\zeta^2)\alpha_1^4\alpha_2^3\alpha_3^2\alpha_5\alpha_6^2 \\
&+ (\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 - 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4\alpha_5\alpha_6 + (\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 - 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4\alpha_5\alpha_6 \\
&+ \frac{1}{2} (2\zeta^5 - \zeta^4 - \zeta^3 + 2\zeta^2 - 3)\alpha_1^3\alpha_2^3\alpha_3^2\alpha_4^2 + (-\zeta^5 - \zeta^4 - \zeta^3 - \zeta^2 + 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5\alpha_6 \\
&+ (-\zeta^5 - \zeta^4 - \zeta^3 - \zeta^2 + 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5\alpha_6 + (\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 - 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5\alpha_6 \\
&+ (-5\zeta^5 - 5\zeta^4)\alpha_1^3\alpha_2^3\alpha_3^2\alpha_4^2\alpha_5^2 + (\zeta^5 - 3\zeta^4 - 3\zeta^3 - 3\zeta^2)\alpha_1^3\alpha_2^3\alpha_3^2\alpha_4^2\alpha_5^2 \\
&+ \frac{1}{2} (-5\zeta^5 - 5\zeta^4 - 5\zeta^3 - 5\zeta^2 + 5)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5^2 \\
&+ (-\zeta^5 - \zeta^2 + 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5^2 + \frac{1}{3} \alpha_1^3\alpha_2\alpha_3^2\alpha_4^2\alpha_5 \\
&+ (-\zeta^5 - \zeta^4 - \zeta^3 - \zeta^2 - 1)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5^2 \\
&+ \frac{1}{2} (2\zeta^5 + 4\zeta^4 + 4\zeta^3 + 2\zeta^2 - 2)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5^2 \\
&+ (2\zeta^5 + 2\zeta^4 + 2\zeta^3 + 2\zeta^2)\alpha_1^3\alpha_2^3\alpha_3\alpha_4^2\alpha_5^2 \\
&+ \frac{1}{117649N^4} \text{Tr}((-2\zeta^5 + 2\zeta^4 + 4\zeta^3 + 8\zeta^2 + 6\zeta + 3)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (-2\zeta^5 + 2\zeta^4 + 4\zeta^3 + 8\zeta^2 + 6\zeta + 3)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (2\zeta^5 + 2\zeta^4 + 4\zeta^3 + 8\zeta^2 + 6\zeta + 3)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (7\zeta^4 + 21\zeta^3 + 28\zeta^2 + 28\zeta + 14)\alpha_1^3\alpha_2^3\alpha_3^2\alpha_4\alpha_5^2 \\
&+ (-7\zeta^5 - 14\zeta^4 - 14\zeta^3 - 21\zeta^2 - 28\zeta - 14)\alpha_1^3\alpha_2^3\alpha_3^2\alpha_4\alpha_5^2 \\
&+ (-7\zeta^4 - 35\zeta^3 - 42\zeta^2 - 42\zeta - 21)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (-14\zeta^5 - 14\zeta^4 - 14\zeta^3 - 14\zeta^2 - 14\zeta - 7)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (7\zeta^5 + 7\zeta^4 - 7\zeta^3 - 21\zeta^2 - 14\zeta - 7)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6 \\
&+ (7\zeta^4 + 21\zeta^3 + 28\zeta^2 + 28\zeta + 14)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5^2 \\
&+ (-21\zeta^5 - 21\zeta^4 + 7\zeta^3 - 7\zeta^2 - 14\zeta - 7)\alpha_1^3\alpha_2\alpha_3\alpha_4^2\alpha_5\alpha_6 \\
&+ (-7\zeta^4 - 7\zeta^3 - 14\zeta^2 - 14\zeta - 7)\alpha_1^3\alpha_2\alpha_3\alpha_4^2\alpha_5\alpha_6 \\
&+ (21\zeta^5 - 42\zeta^4 - 63\zeta^3 - 21\zeta^2 - 42\zeta - 21)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5^2 \\
&+ (42\zeta^5 + 63\zeta^4 + 21\zeta^3 + 42\zeta^2 + 84\zeta + 42)\alpha_1^3\alpha_2\alpha_3^2\alpha_4^2\alpha_5 \alpha_6 \\
&+ (7\zeta^5 + 7\zeta^4 - 7\zeta^3 - 7\zeta^2)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2 + (-21\zeta^5 + 21\zeta^4)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2 \\
&+ (14\zeta^5 + 28\zeta^4 + 35\zeta^3 + 28\zeta + 14)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2 \\
&+ (-14\zeta^5 + 14\zeta^4 + 42\zeta^3 + 70\zeta^2 + 56\zeta + 28)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2 \\
&+ (-35\zeta^5 + 35\zeta^4 - 70\zeta^2 - 70\zeta - 35)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2 \\
&+ (14\zeta^3 + 14\zeta^2 + 14\zeta + 7)\alpha_1^3\alpha_2\alpha_3^2\alpha_4\alpha_5\alpha_6^2
\end{align*}\]
+ (-14\zeta^5 + 14\zeta^2)\alpha_1^4\alpha_2^2\alpha_3\alpha_4^2\alpha_6^3
+ (14\zeta^5 + 14\zeta^4 + 14\zeta^3 + 14\zeta^2 + 28\zeta + 14)\alpha_1^3\alpha_2^3\alpha_3^3\alpha_4^2\alpha_6^2)

where Tr is the trace map from \(\mathbb{Q}(\zeta)\) to \(\mathbb{Q}\) and \(N = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha_1)\). Therefore, \(F(X)\) is, in fact, a polynomial in \(\mathbb{Q}[u_1, u_2, u_3, u_4, u_5, u_6][X]\).

There are other examples found by computer search:

\[
\begin{align*}
n &= 10, & m &= 11, & \mathcal{P}(t) &= -t^5 - t^2 + t, \\
n &= 8, & m &= 35, & \mathcal{P}(t) &= -t^7 + t^3 + t.
\end{align*}
\]

In particular, the former polynomial enables us to classify the cyclic extensions of degree 11 over \(\mathbb{Q}\).

5. From \(R_{K/k}\mathbb{G}_m\) to \(R_{K/k}^{(1)}\mathbb{G}_m\)

In this section, we shall show the following theorem that relates the Kummer theories for \(R_{K/k}\mathbb{G}_m\) and \(R_{K/k}^{(1)}\mathbb{G}_m\).

**Theorem 5.1.** If an endomorphism \(\lambda\) of \(R_{K/k}\mathbb{G}_m\) induces a Kummer duality

\[
\kappa_k : R_{K/k}\mathbb{G}_m(k)/\lambda R_{K/k}\mathbb{G}_m(k) \sim \text{Hom}_{\text{cont}}(\text{Gal}(\overline{k}/k), \ker \lambda(\overline{k}))
\]

then \(\lambda' = \lambda|_{R_{K/k}\mathbb{G}_m}\) is an endomorphism of \(R_{K/k}^{(1)}\mathbb{G}_m\) and induces a Kummer duality

\[
\kappa_k^{(1)} : R_{K/k}^{(1)}\mathbb{G}_m(k)/\lambda R_{K/k}^{(1)}\mathbb{G}_m(k) \sim \text{Hom}_{\text{cont}}(\text{Gal}(\overline{k}/k), \ker \lambda(\overline{k}))
\]

**Proof.** We shall first show that \(\lambda' = \lambda|_{R_{K/k}\mathbb{G}_m}\) is an endomorphism of \(R_{K/k}^{(1)}\mathbb{G}_m\). Suppose that \(\lambda\) is associated to a circulant matrix \(\text{circ}(c_1, \ldots, c_n)\). We first fix isomorphisms \(\phi : R_{K/k}\mathbb{G}_m \cong \mathbb{G}_m^n, k\) and \(\psi : R_{K/k}^{(1)}\mathbb{G}_m \cong \mathbb{G}_m^{n-1}\) defined over the splitting field \(K\) such that the following diagram is commutative with exact rows:

\[
\begin{array}{cccccc}
1 & \longrightarrow & R_{K/k}^{(1)}\mathbb{G}_m & \longrightarrow & R_{K/k}\mathbb{G}_m & \longrightarrow & \mathbb{G}_m^n, k & \longrightarrow & 1 \\
\psi & & \downarrow \phi & & \downarrow & & \downarrow N & & \\
1 & \longrightarrow & \mathbb{G}_m^{n-1, K} & \longrightarrow & \mathbb{G}_m^n, K & \longrightarrow & \mathbb{G}_m, k & \longrightarrow & 1
\end{array}
\]

The bottom exact row is induced by the map

\[
N : (X_1, \ldots, X_n) \mapsto \prod_{i=1}^n X_i.
\]

Let \(X = (X_1, \ldots, X_n)\) be a point in the kernel of \(\psi\). Namely we have \(\prod_{i=1}^n X_i = 1\). Then the image of \(X\) under \(\lambda\) is given by (3.1) and the product of the coordinates of the image is
\[
\prod_{j=1}^{n} X_j^{c_j} X_j^{c_j - 1} \cdots X_j^{c_j - n + 1} = \prod_{j=1}^{n} X_j^{\sum_{k=1}^{n} c_j - k + 1}
\]

with the cyclic notation. Each exponent is equal to \(c_1 + \cdots + c_n\). Consequently the above product equals to
\[
\left( \prod_{j=1}^{n} X_j \right)^{c_1 + \cdots + c_n} = 1.
\]

This shows that the image is also in the kernel of \(N\). Hence the image of \(\lambda'\) lies in \(R^{(1)}_{K/k} G_m\). In particular, we have \(\ker \lambda'(\bar{k}) \subset \ker \lambda(\bar{k})\).

Now we consider the following commutative diagram of \(k\)-schemes with exact rows and columns:

We shall compute \(\mu\) in the diagram explicitly. Taking the dual, we have a commutative diagram with exact columns (see [13, §4.8]):

Here the vertical map \(Z \to \mathbb{Z}[G]\) is defined by \(1 \mapsto \sum_{g \in G} g\). Hence we have \(A(\sum g) = \sum_g (\sum_{j=1}^{n} c_j)\). This means that the map \(M\) is the multiplication-by-(\(c_1 + \cdots + c_n\)) map. We conclude that \(\mu\) is the \((c_1 + \cdots + c_n)\)-th power map. By the assumption \(c_1 + \cdots + c_n = \pm 1\), we have \(\ker \mu = 1\). It yields \(\ker \lambda \equiv \ker \lambda'\). In particular, the degrees of \(\lambda\) and \(\lambda'\) are the same.

Since \(\lambda' R^{(1)}_{K/k} G_m(k) \subset \lambda R_{K/k} G_m(k)\), we have a well-defined homomorphism from \(R^{(1)}_{K/k} G_m(k) / \lambda' R^{(1)}_{K/k} G_m(k)\) to \(R_{K/k} G_m(k) / \lambda R_{K/k} G_m(k)\) and this homomorphism fits in the commutative diagram with exact rows:
Suppose that $\lambda$ induces a Kummer duality $\kappa_k$. Then we have $\ker \lambda'(\bar{k}) \subset \ker \lambda(\bar{k}) = \ker \lambda(k)$. It follows that $\ker \lambda'(\bar{k}) = \ker \lambda'(k)$. Also by taking the Galois cohomology of the exact sequence

$$1 \longrightarrow R^{(1)}_{K/k} G_m(k)/\lambda' R^{(1)}_{K/k} G_m(k) \longrightarrow H^1(k, \ker \lambda') \longrightarrow H^1(k, R^{(1)}_{K/k} G_m)[\lambda'] \longrightarrow 1,$$

we obtain

$$R_{K/k} G_m(k) \xrightarrow{\text{Norm}} G_{m,k}(k) \longrightarrow H^1(k, R^{(1)}_{K/k} G_m) \longrightarrow 1.$$

By the argument in [5, Section 4], we have

$$H^1(k, R^{(1)}_{K/k} G_m) \cong k^\times / N_{K/k} K^\times$$

and, since $(\deg \lambda', n) = (\deg \lambda, n) = 1$, we conclude

$$H^1(k, R^{(1)}_{K/k} G_m)[\lambda'] = 1.$$

Finally we obtain a Kummer duality

$$\kappa^{(1)}_k : R^{(1)}_{K/k} G_m(k)/\lambda' R^{(1)}_{K/k} G_m(k) \xrightarrow{\sim} \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda'(\bar{k}))$$

as expected. This proves the theorem. $\square$

The Kummer theory of $R_{K/k} G_m$ always has one more dimension than that of $R^{(1)}_{K/k} G_m$. This is certainly a disadvantage for the Kummer theory of $R_{K/k} G_m$. But according to this theorem, we can always reduce this extra dimension. Therefore, it is a nice idea to work with $R_{K/k} G_m$ for finding a Kummer duality, then move to $R^{(1)}_{K/k} G_m$ to compute explicit polynomials.

6. Relation between descent Kummer theories

Throughout this section, we use the following setting and notation. Let $k$ be a field and $K = k(\zeta_n)$. We set $n = [K : k]$. We fix an isomorphism $\phi_k : R_{K/k} G_m \cong G_{m,k}^n$ over $K$. Suppose that $K/k$ satisfies the assumptions of Theorem 1.1. Then there exists an endomorphism $\lambda$ of $R_{K/k} G_m$ of degree $m$ corresponding to a circulant matrix $\Lambda = \text{circ}(c_1, \ldots, c_n)$ and $\lambda$ induces a Kummer duality $\kappa_k$ in (1.5).

Our main result in this section is the following theorem on base change.

**Theorem 6.1.** Let $k'$ be an intermediate field of $K/k$. Then there exists an endomorphism $\lambda'$ on $R_{K/k'} G_m$ of degree $m$ that induces a Kummer duality

$$\kappa_{k'} : R_{K/k'} G_m(k')/\lambda' R_{K/k'} G_m(k') \xrightarrow{\sim} \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k'), \ker \lambda'(\bar{k})).$$

(6.1)
Moreover there exists a homomorphism
\[ \rho_{k \to k'} : R_{K/k} \mathbb{G}_m(k)/ \lambda R_{K/k} \mathbb{G}_m(k) \to R_{K'/k'} \mathbb{G}_m(k')/ \lambda' R_{K'/k'} \mathbb{G}_m(k') \]  
(6.2)
such that
\[ k^\ker \kappa' (\rho_{k \to k'}(P)) = k'^\ker \kappa (P) \]  
(6.3)
holds for all \( P \in R_{K/k} \mathbb{G}_m(k) \).

We first show the existence of an endomorphism \( \lambda' \) satisfying (6.1). To do this, we construct an endomorphism \( \Lambda' = \circ(b_1, \ldots, b_{n'}) \) of the character module of \( R_{K/k} \mathbb{G}_m \) form \( \Lambda = \circ(c_1, \ldots, c_n) \). Here we let \( n' = [K : k'] \).

Set \( d = n/n' = [k' : k] \). Then \( \zeta_n^i \ (i = 0, 1, \ldots, n' - 1) \) form a complete set of representatives of the group \( \mu_n \) modulo \( \mu_d \). Let \( \mathcal{P}(t) \) be the representer of \( \Lambda \). We define
\[ \mathcal{I}(t) = \prod_{v \in \mu_d} \mathcal{P}(vt). \]

We need the following lemma.

**Lemma 6.2.** The polynomial \( \mathcal{I}(t) \) is a polynomial in \( t^d \) with integer coefficients.

**Proof.** By the definition of \( \mathcal{I}(t) \) and the fact \( \mathcal{P}(t) \in \mathbb{Z}[t] \), we obviously have \( \mathcal{I}(t) \in \mathbb{Z} [\mu_d][t] \). Let \( s \) be any element of \( \text{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}) \). Then \( s \) permutes the elements of \( \mu_d \). Thus we have
\[ \mathcal{I}(t)^s = \prod_{v \in \mu_d} \mathcal{P}(v^s t) = \prod_{v \in \mu_d} \mathcal{P}(vt) = \mathcal{I}(t). \]
This implies \( \mathcal{I}(t) \in \mathbb{Z}[t] \).

To prove that \( \mathcal{I}(t) \) is a polynomial in \( t^d \), it suffices to show \( \mathcal{I}(\xi t) = \mathcal{I}(t) \) for all \( \xi \in \mu_d \). As a matter of fact, we have
\[ \mathcal{I}(\xi t) = \prod_{v \in \mu_d} \mathcal{P}(\xi vt) = \prod_{v \in \mu_d} \mathcal{P}(vt) = \mathcal{I}(t). \]
This completes the proof of the lemma. \( \square \)

Now we shall show that a new polynomial \( \mathcal{Q}(t) = b_1 + b_2 t + \cdots + b_n t^{n' - 1} \) of degree \( n' - 1 \) is uniquely determined by the condition
\[ \mathcal{Q}(\zeta_n^i) = \mathcal{I}(\zeta_n^i) \quad (i = 0, 1, \ldots, n' - 1). \]  
(6.4)
Note here that, since \( \mathcal{I}(t) \) is a polynomial in \( t^d \), \( \mathcal{I}(\zeta_n^i) \) is a polynomial in \( \zeta_n^d \). In terms of matrices, the above Eqs. (6.4) become
\[
\begin{bmatrix}
1 & 1 & \cdots & 1 \\
1 & \zeta_n^d & \cdots & \zeta_n^{d(n' - 1)} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \zeta_n^{d(n' - 1)} & \cdots & \zeta_n^{d(n' - 1)(n' - 1)}
\end{bmatrix}
\begin{bmatrix}
b_1 \\
b_2 \\
\vdots \\
b_{n'}
\end{bmatrix}
= \begin{bmatrix}
\mathcal{I}(1) \\
\mathcal{I}(\zeta_n) \\
\vdots \\
\mathcal{I}(\zeta_n^{n' - 1})
\end{bmatrix}.
\]
Let us denote the $n' \times n'$ matrix on the left hand side by $F$. The matrix $F$ is essentially a Fourier matrix. We multiply $F^* = [\zeta_n^{-d(i-1)(j-1)}]$ on the both sides of the above equation. A simple computation yields

$$n' \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n'} \end{bmatrix} = F^* \begin{bmatrix} \mathcal{X}(1) \\ \mathcal{X}(\zeta_n) \\ \vdots \\ \mathcal{X}(\zeta_n^{n'-1}) \end{bmatrix}. \quad (6.5)$$

It remains to show that every entry of the right hand side of (6.5) is an integer multiple of $n'$. By Lemma 6.2, we can write $\mathcal{X}(t) = \sum_{i=0}^{n-1} s_i t^d$ with integer coefficients $s_i$. The $j$-th entry of the right hand side is

$$\sum_{k=1}^{n'} \zeta_n^{-d(j-1)(k-1)} \sum_{i=0}^{n-1} s_i \zeta_n^{(k-1)d} = \sum_{i=0}^{n-1} s_i \sum_{k=1}^{n'} \zeta_n^{(k-1)(i-j+1)}.$$

The inner sum is $n'$ if $i-j+1 \equiv 0 \pmod{n'}$ and 0 otherwise. Thus it becomes

$$\sum_{i=0}^{n-1} n's_i.$$

This shows the existence of $\mathcal{D}(t) \in \mathbb{Z}[t]$ satisfying (6.4).

Let $\lambda'$ be the endomorphism of $R_{K'/\mathbb{Q}_m}$ induced from the circulant matrix whose representer is $\mathcal{D}(t)$. Then, by (6.4), the degree of $\lambda'$ is equal to that of $\lambda$. Indeed, we have

$$\deg \lambda' = |\det(\text{circ}(b_1, \ldots, b_{n'}))| = \prod_{i=0}^{n'-1} \mathcal{D}(\zeta_n^i) = \prod_{i=0}^{n'-1} \mathcal{X}(\zeta_n^i) = \prod_{i=0}^{n'-1} \mathcal{X}(\nu_{\zeta_n^i}) = \prod_{\zeta \in \mu_n} \mathcal{P}(\zeta) = m.$$

We write

$$\mathcal{D}(\zeta_n^i) = \mathcal{X}(\zeta_n^i) = \prod_{j=0}^{d-1} \mathcal{P}(\zeta_n^{j+i}).$$

If $(i, n') > 1$, then we have $\mathcal{D}(\zeta_n^i) \in (\mathbb{Z}[\zeta_n^i])^\times = (\mathbb{Z}[\zeta_n])^\times$. On the other hand, if $i = 1$, then the set of $n'j+1$ $(j = 0, \ldots, d-1)$ contains all the representatives of $(\mathbb{Z}/n)^\times$ that are congruent to 1 modulo $n$. This means that the product $\prod \mathcal{P}(\zeta_n^{n'j+i})$ is divided by the norm $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)} \mathcal{P}(\zeta_n)$. By considering the absolute value of the product, the difference between them must be a unit. Therefore, $\mathcal{D}(\zeta_n^i)$ and $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)} \mathcal{P}(\zeta_n)$ generate a same ideal in $\mathbb{Z}[\zeta_n]$. Since the prime ideals dividing $\mathcal{P}(\zeta_n)$ are of degree one, we conclude $\mathbb{Z}[\zeta_n]/(\mathcal{D}(\zeta_n^i)) \cong \mathbb{Z}/(m)$. Since the ideal $(\mathcal{P}(\zeta_n))$ of $\mathbb{Z}[\zeta_n]$ is lying above $(\mathcal{D}(\zeta_n^i))$ of $\mathbb{Z}[\zeta_n]$, we have a natural isomorphism from $\mathbb{Z}[\zeta_n]/(\mathcal{D}(\zeta_n^i))$ to $\mathbb{Z}[\zeta_n]/(\mathcal{P}(\zeta_n))$. We can define $\nu_{\zeta_n^i}$ so that it makes the following diagram commutative:
\[
\begin{array}{c}
\text{Gal}(K/k) \xrightarrow{v_k} \langle \xi_n \mod \mathcal{P} \rangle \\
\text{natur inc.} \downarrow \quad \downarrow \\
\text{Gal}(K/k') \xrightarrow{v_{k'}} \langle \xi_{n'} \mod \mathcal{P}' \rangle.
\end{array}
\]

(6.6)

We have shown that \(\mathcal{P}(t)\) satisfies the conditions of Theorem 1.1 and thus it induces a Kummer duality \(\kappa'\) in (6.1).

The next step is to define a group homomorphism \(\rho_{k \to k'}\) in (6.2). Let \(\tau\) be an element of \(\text{Gal}(K/k)\) satisfying \(v_k(\tau) = (\xi_n \mod \mathcal{P})\) by the isomorphism (1.4). We define an \(n' \times n\) matrix \(R\) by

\[
R = \frac{1}{n} \begin{bmatrix}
v_k(1) & v_k(\tau) & \ldots & v_k(\tau^{n-1}) \\
v_k(\tau^d) & v_k(\tau^{d+1}) & \ldots & v_k(\tau^{n-d-1}) \\
& \ldots & \ldots & \ldots \\
v_k(\tau^{d^m}) & v_k(\tau^{d^m+1}) & \ldots & v_k(\tau^{d^n})
\end{bmatrix}.
\]

Since \(n\) is invertible modulo \(m\), the matrix \(R\) is well defined as a matrix over \(\mathbb{Z}/m\mathbb{Z}\). The matrix \(R\) is obtained by shifting each previous row by \(d\) positions to the right. We should bear in mind that any \(\text{Gal}(K/k')\)-module homomorphism \(\mathbb{Z}[\text{Gal}(K/k')] \to \mathbb{Z}[\text{Gal}(K/k)]\) is given by a matrix of this form with integer entries. We consider that \(R\) is obtained by reducing such an integer matrix modulo \(m\). We define \(\rho_{k \to k'}\) as a \(\mathbb{Z}/m\mathbb{Z}\)-module homomorphism induced by \(R\). To show \(\rho_{k \to k'}\) is well defined, we have only to show that \(RA \equiv 0\) (mod \(m\)) because the quotient group in the left hand side of \(k\) has exponent \(m\). Since the \((i, k)\)-entry of \(R\) is \(v_k(\tau^{-(k+1)+(i-1)d})\) and the \((k, j)\)-entry of \(A\) is \(n_{j-k+1}\), the \((i, j)\)-entry of \(RA\) is

\[
\sum_{k=1}^{n} v_k(\tau^{-(k+1)+(i-1)d})c_{j-k+1} = v_k(\tau^{-(j-2+(i-1)d)}) \sum_{k=1}^{n} v_k(\tau^{j-k+1})c_{j-k+1} = v_k(\tau^{-(j-2+(i-1)d)}) \mathcal{P}(v_k(\tau)) \equiv 0 \quad (\text{mod } m).
\]

Here the last congruence follows from (1.2). This proves the assertion.

Finally we shall show that the equality (6.3) holds. For every \(P \in R_{K/k}G_m(k)\), the field \(L_P = k\ker \kappa_P\) is a cyclic extension over \(k\) of degree \(m\). The field extension \(KL_P/K\) is a Kummer extension in the classical sense. Thus we can find an element \(a\) of \(K^\times\) satisfying \(KL_P = K(\sqrt[m]{a})\). The following proposition tells us how to choose a Kummer generator \(a\).

**Proposition 6.3.** Let the notations be as above. Define \(e(K/k) \in \mathbb{Z}/m\mathbb{Z}[\tau]\) by

\[
e(K/k) = \frac{1}{n} \sum_{i=0}^{n-1} v_k(\tau^{-i}) \tau^i,
\]

where \(v_k\) is the isomorphism in (1.4). Let \(\phi_k(P) = (\alpha_1, \ldots, \alpha_n)\). Then we have

\[
KL_P = K(\sqrt[m]{\epsilon(K/k)}).
\]

**Proof.** First observe that \(\alpha_1, \ldots, \alpha_n\) are the elements of \(K\) since \(P\) is a \(k\)-rational point. Let \(Q\) be a point in \(R_{K/k}G_m(k)\) such that \(\lambda(Q) = P\). If we write \(\phi_k(Q) = (X_1, \ldots, X_n)\), then we have

\[
(\alpha_1, \ldots, \alpha_n) = \Lambda(X_1, \ldots, X_n).
\]

(6.7)
It is easy to see that $KL_P = K(X_1, \ldots, X_n)$ holds. Let $H$ be the row reduced lower triangular Hermite normal form of $\Lambda$, which is obtained by reducing the rows from the bottom. Let $V = [v_{ij}]$ be a transformation matrix. Then we have

$$H = \begin{bmatrix} m & 0 & 0 & 0 \\ \ast & 1 & 0 & \ast \\ \ast & \ast & \ast & 0 \\ \ast & \ast & \ast & 1 \end{bmatrix} = V \Lambda,$$

since $\Lambda$ has a cyclic cokernel of order $m$. Multiplying $V$ from the left on the both sides of (6.7), we obtain

$$V(\alpha_1, \ldots, \alpha_n) = H(X_1, \ldots, X_n).$$

Comparing the first entries of the both sides, we have

$$X_1^m = \alpha_1^{\nu_{11}} \cdots \alpha_n^{\nu_{1n}}.$$

By using the other entries from the top, $X_i \ (i = 2, \ldots, n)$ are expressed in terms of $\alpha_i$'s and $X_1$. Hence $KL_P$ is generated only by $X_1$ over $K$: $KL_P = K(X_1)$. It follows from (6.8) that the row vector $[v_{11}, \ldots, v_{1n}]$ is a solution of a linear congruence

$$c_1 v_{11} + c_n v_{12} + \cdots + c_2 v_{1n} \equiv 0 \pmod{m}.$$  

On the other hand, we notice

$$\mathcal{P}(\zeta_n) = \mathcal{P}(v_k(\tau)) = c_1 + c_2 v_k(\tau) + \cdots + c_n v_k(\tau^{n-1}) \equiv 0 \pmod{m}$$

by (1.2). Since it is known that $v_{11}, \ldots, v_{1n}$ are uniquely determined modulo $m$, these two equations yield $v_{1i} \equiv v_k(\tau^{-i+1}) \pmod{m}$. Hence in $K^\times/(K^\times)^m$ we have

$$\alpha_1^{v_{11}} \cdots \alpha_n^{v_{1n}} = \alpha_1^{v_k(1) + n v_k(\tau^{-1}) + \cdots + n v_k(\tau^{-(n-1)})} = \alpha_1^{ne(K/k)}.$$

Since $n$ is prime to $m$, it follows from [2, Corollary 10.2.7] that

$$KL_P = K(X_1) = K(\sqrt[ne(K/k)]{\alpha_1})$$

as required.  

Usually in the classical theory, we construct a Kummer generator by using a Lagrange resolvent [2, Theorem 5.3.5(5)] and we loose various information through this procedure, since the resolvent is a sum. On the other hand, our Kummer generator is a product of quantities closely related to the parameter $P$ and it preserves such information (see Corollary 6.4).

We think over a reverse situation of Proposition 6.3 in brief. That is to say, suppose that we are given a Kummer extension $K(\sqrt[ne(K/k)]{\gamma})$ over $K$. If there exists a cyclic extension of $L$ over $k$ of degree $m$ satisfying $KL = K(\sqrt[ne(K/k)]{\gamma})$, we can take a generator satisfying $\gamma e(K/k) \equiv \gamma \pmod{(K^\times)^m}$ by Proposition 6.3. It follows from the proposition that an inverse image of $P = R_{K/k}(\gamma') \in R_{K/k}\mathbb{G}_m(k)$ under $\lambda$ generates $L$. Compare this remark with Cohen’s result [2, Theorem 5.3.5] and Nakano’s result [9, Proposition 1], where they take a trace of an element as a generator of $L$. 
We shall now resume the proof of Theorem 6.1. Let \( P' = \rho_{k' \rightarrow k'}(P) \) and \( L_{P'} = \ker_{k'}(P') \). We apply Proposition 6.3 also to \( L_{P'} \). From the definition of \( R \) corresponding to \( \rho_{k \rightarrow k'} \), we see \( \phi_{k'}(P') = (\alpha_1^{e(K/k)}, \alpha_{d+1}^{e(K/k)}, \ldots, \alpha_{(n'-1)d+1}^{e(K/k)}) \). Thus we have

\[
KL_{P'} = K\left( \sqrt[n']{\alpha_1^{e(K/k)}e(K/k')} \right),
\]

where \( e(K/k') \) is similarly defined by

\[
e(K/k') = \frac{1}{n'} \sum_{j=0}^{n'-1} v_{k'}(\tau^{-dj}) \tau^{dj}.
\]

Note that \( \tau^d \) is a generator of \( \text{Gal}(K/k') \). If we can show \( KL_P = KL_{P'} \), then an easy application of Galois theory implies our claim (6.3). Therefore it remains to show

\[
\langle \alpha_1^{e(K/k)} \rangle = \langle \alpha_1^{e(K/k)}e(K/k') \rangle
\]

in \( K^\times/(K^\times)^m \). It suffices to prove that

\[
e(K/k) = e(K/k)e(K/k').
\]

By (6.6) we have \( v_{k'}(\tau^d) = v_k(\tau^d) \). Writing \( i = dj + r \) \((r = 0, \ldots, d-1, j = 0, \ldots, n'-1)\), we rewrite \( e(K) \) as

\[
e(K/k) = \frac{1}{n} \sum_{r=0}^{d-1} \sum_{j=0}^{n'-1} v_k(\tau^{-dj}) v_k(\tau^{-r}) \tau^{dj} \tau^r = e(K/k') \frac{1}{d} \sum_{r=0}^{d-1} v_k(\tau^{-r}) \tau^r.
\]

Since \( e(K/k') \) is an idempotent, we have

\[
e(K/k)e(K/k') = e(K/k') \frac{1}{d} \sum_{r=0}^{d-1} v_k(\tau^{-r}) \tau^r = e(K/k') \frac{1}{d} \sum_{r=0}^{d-1} v_k(\tau^{-r}) \tau^r = e(K/k).
\]

This completes the proofs of the claim and Theorem 6.1. \( \square \)

The following two corollaries are obtained from Proposition 6.3. Thus suppose that we are in the same situation as in the proposition.

**Corollary 6.4.** Assume that \( k \) is a global field. Then the cyclic extension \( L_P/k \) is unramified outside the primes dividing \( \alpha_i \) and \( m \).

**Proof.** Since \([K:k]\) and \([L_P:k]\) are relatively prime, the decomposition law in \( L/k \) is essentially determined by that of \( KL_P/K \). Now the corollary follows from a well-known ramification property of Kummer extensions (see, for example, [2, Theorem 10.2.9]). \( \square \)

For an explicit example of the decomposition law in the case of norm tori, see [6, Theorem 3].
Corollary 6.5. Let $P_1, P_2 \in R_{K/k}\mathbb{G}_m(k)$ and $\phi_k(P_1) = (\alpha_1, \ldots, \alpha_n), \phi_k(P_2) = (\beta_1, \ldots, \beta_n)$. Then the fields $L_{P_1}$ and $L_{P_2}$ are isomorphic if and only if $\alpha_1^{e(K/k)}$ and $\beta_1^{e(K/k)}$ generate a same group modulo $(K^\times)^m$.

Proof. The field $L_{P_1}$ (resp. $L_{P_2}$) is a unique intermediate field of degree $m$ over $k$ inside $K(\sqrt[m]{\alpha_1^{e(K/k)}})$ (resp. $K(\sqrt[m]{\beta_1^{e(K/k)}})$). The corollary follows immediately from [2, Corollary 10.2.7(2)] and Proposition 6.3. □

This type of result is useful to classify parametric polynomials (in the sense of [4, Definition 0.11]). Such an example dealing with Brumer’s quintic polynomials is found in [7]. It is also useful to construct an isomorphic family of polynomials with different parameters. Since an isomorphic class is determined only by the $e(K/k)$-component, multiplying other component does not influence the isomorphism class.

We conclude with a few explicit examples of the applications of Theorem 6.1.

Example 6.6. In this example, we write $\zeta = \zeta_5$ for short. Let $k = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta)$. Therefore, we have $m = 5$ and $n = 4$. By Example 4.3, $\Lambda = \text{circ}(1,1,-1,0)$ induces a Kummer duality. The representer is $\mathcal{P}(t) = 1 + t - t^2$. Since $\sqrt{-1} \equiv 3 \pmod{\mathcal{P}(\sqrt{-1})}$, the automorphism $\tau : \zeta \mapsto \zeta^3$ is a generator of $\text{Gal}(K/k)$. Hence we have $v_k(\tau) = 3 \mod 5$. Let $K' = \mathbb{Q}(\sqrt{5})$ be the unique quadratic subfield of $K$. We compute

$$\mathcal{I}(t) = \mathcal{P}(t)\mathcal{P}(-t) = 1 - 3t^2 + t^4.$$ 

A linear polynomial representer $\mathcal{L}$ must satisfy $\mathcal{L}(1) = \mathcal{I}(1) = -1$ and $\mathcal{L}(-1) = \mathcal{I}(\sqrt{-1}) = 5$. It follows that $\mathcal{L}(t) = 2 - 3t$. We have $v_k(\tau^2) = v_k(\tau^2) = 4 \mod 5$. This $\mathcal{L}(t)$ defines an endomorphism of $R_{K/k}\mathbb{G}_m$ of degree 5 by Theorem 6.1 that induces a Kummer duality $\kappa_k$. The map $\rho_k \rightarrow \kappa$ is determined by

$$R = \frac{1}{4} \begin{bmatrix} 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 4 & 3 \end{bmatrix}.$$ 

Define $\phi_k : R_{K/k}\mathbb{G}_m \rightarrow \mathbb{G}_m^4$ by

$$(u_1, u_2, u_3, u_4) \mapsto (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

where

$$\alpha_i = (u_1 \zeta + u_2 \zeta^3 + u_3 \zeta^4 + u_4 \zeta^5)^{\tau^{i-1}}$$

for $i = 1, 2, 3, 4$. By Proposition 6.3 we have $KL = K(\sqrt[5]{\alpha_1^{e(K/k)}})$ with $e(K/k) = 4 + 2\tau^3 + \tau^2 + 3\tau$.

Next let us change the notation. Let $k = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{P}(t) = 2 - 3t$. We consider the case where $K = K'$. We calculate $\mathcal{J}(t) = 4 - 9t^2$ and $\mathcal{L}(t) = -5$. The $(5)-$th power map on $R_{K/k}\mathbb{G}_m = \mathbb{G}_{m,K}$ is obviously induces the classical Kummer theory.

Example 6.7. Let $K = \mathbb{Q}(\zeta_7), k = \mathbb{Q}$, and $K' = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. We have a Kummer duality for $R_{K/k}\mathbb{G}_m$ with $\mathcal{P}(t) = t - t^3 - t^4$ as shown in Example 4.4. We denote $(-1 + \sqrt{-3})/2$ by $\omega$. Then we have

$$\mathcal{J}(t) = \mathcal{P}(t)\mathcal{P}(\omega t)\mathcal{P}(\omega^2 t) = -t^{12} + 2t^{12} - 3t^{16} + t^{13}.$$
and the corresponding linear representer $Q(t)$ for $R_{K/k}\mathbb{G}_m$ must satisfy $Q(1) = I(1) = -1$ and $Q(-1) = I(\zeta_6) = -1$. Therefore we obtain $Q(t) = -4 + 3t$. The polynomial $Q(t)$ agrees with the polynomial obtained from Example 4.2 by letting $m = 7$ up to the sign. Note that $-1$ induces an automorphism of $R_{K/k}\mathbb{G}_m$.

We use a computer algebra system MAGMA [1] for the computation of the examples in this paper.

References