Bull. Aust. Math. Soc. **96** (2017), 196–204
doi:10.1017/S0004972717000491

RAMIFICATION IN KUMMER EXTENSIONS ARISING FROM ALGEBRAIC TORI

MASAMITSU SHIMAKURA

(Received 4 November 2016; accepted 7 April 2017; first published online 17 August 2017)

Abstract

We describe the ramification in cyclic extensions arising from the Kummer theory of the Weil restriction of the multiplicative group. This generalises the classical theory of Hecke describing the ramification of Kummer extensions.

2010 *Mathematics subject classification*: primary 11S15.

Keywords and phrases: local field, ramification, algebraic tori.

1. Introduction

Let p be a fixed odd prime. Let $\mathbb{Q}_p$ be the field of p-adic numbers and $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$. We assume that any algebraic extensions of $\mathbb{Q}_p$ are contained in $\overline{\mathbb{Q}}_p$. Let l be an odd prime and denote by ζ_l a primitive lth root of unity in $\overline{\mathbb{Q}}_p$. Let k be an unramified extension of $\mathbb{Q}_p$ of degree n and $k_z = k(\zeta_l)$. Let K be an intermediate field of k_z/k and T the Weil restriction $R_{k_z/K}\mathbb{G}_m$ of the multiplicative group $\mathbb{G}_m$ to K. We assume that there exists a self-isogeny λ on T of degree l whose kernel $\mathrm{Ker}\lambda$ is contained in the group $T(K)$ of K-rational points of T. Several conditions for the existence of such λ are given in [3] along with several examples. Under this assumption, we have the isomorphism

$$\kappa_K : T(K)/\lambda T(K) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{K}/K), \mathrm{Ker}\lambda(\overline{K}))$$

proved by Kida [3]. Here $\overline{K}$ is an algebraic closure of K in $\overline{\mathbb{Q}}_p$ and the right-hand side is the group of continuous homomorphisms. The case $K = k_z$ is the classical Kummer theory. The general case is an extension of the Kummer theory for fields without roots of unity. In particular, any cyclic extension of degree l over K can be written as $K(\lambda^{-1}(P))$ with $P \in T(K)$. In this paper, we determine the ramification in $L = K(\lambda^{-1}(P))$ over K.

In the case where K is a finite extension of $k = \mathbb{Q}(\zeta_l + \zeta_l^{-1})$, the ramification in the cyclic extension L/K is studied by Komatsu [4] using an algebraic torus of dimension 1 which consists of the kernel of the norm map in a quadratic extension. We shall generalise his result to the case $\zeta_l + \zeta_l^{-1} \notin K$. Since the problem is obviously local, we assume that the base field K is a local field.

The following notations will be used throughout this paper. Let v_{k_z} (respectively v_K) be the discrete valuation of k_z (respectively K), normalised by $v_{k_z}(k_z^\times) = \mathbb{Z}$ (respectively $v_K(K^\times) = \mathbb{Z}$). Let $U(k_z)$ be the group of units in k_z defined by

$$U(k_z) = \{u \in k_z \mid v_{k_z}(u) = 0\}, \tag{1.1}$$

and $U^{(i)}(k_z)$ the groups of higher principal units defined by

$$U^{(i)}(k_z) = \{u \in k_z \mid v_{k_z}(u-1) \geq i\}, \quad i \in \mathbb{N}. \tag{1.2}$$

Our main theorem can be stated as follows.

THEOREM 1.1 (see Theorem 3.2). *Let $p = l$ be an odd prime. Let m be the degree of the extension K/k. Let $\widehat{T} = \mathrm{Hom}(T, \mathbb{G}_{m,k_z})$ be the group of characters of T. For each $i \geq 1$, set $T^{(i)}(K) = \mathrm{Hom}_{\mathrm{Gal}(k_z/K)}(\widehat{T}, U^{(i)}(k_z))$. If $P \in T^{(jd+1)}(K)$ and $P \notin T^{(jd+2)}(K)$ for some j with $0 \leq j \leq m$, then the conductor $\mathfrak{f}$ of $K(\lambda^{-1}(P))/K$ satisfies*

$$v_K(\mathfrak{f}) = \begin{cases} m - j + 1 & \text{for } 0 \leq j < m, \\ 0 & \text{for } j = m. \end{cases}$$

In particular, $K(\lambda^{-1}(P))/K$ is an unramified extension if and only if $P \in T^{(l)}(K)$.

Using this theorem, we can calculate the number of cyclic extensions of degree l over K with a given conductor $\mathfrak{f}$ up to isomorphism in $\overline{\mathbb{Q}}_p$ (see Theorem 3.3).

The outline of the paper is as follows. In Section 2, we discuss the $\mathrm{Gal}(k_z/K)$-module structure of $S_l(k_z^\times) = k_z^\times/(k_z^\times)^l$ and determine the structure of S_1^K which is a certain eigenspace of $S_l(k_z^\times)$. In Section 3, we prove the main theorem using Hecke's theorem [1], which describes the ramification in a cyclic extension of k_z.

REMARK 1.2. When $l \mid p^n - 1$, we can use the classical Kummer theory since $K = k_z$. Therefore, we may assume the condition $l \nmid p^n - 1$. Theorem 1.1 deals with the difficult case $p = l$. For the easier case with $p \neq l$, see Proposition 3.6.

2. Galois module structure of $S_l(k_z^\times)$

Let $p = l$ be an odd prime and k an unramified extension of $\mathbb{Q}_l$ of degree n. We denote by k_z the field $k(\zeta_l)$ as above. Let K be an intermediate field of k_z/k of degree m over k. Set $d = (l-1)/m$. The Galois groups $\mathrm{Gal}(k_z/k)$ and $\mathrm{Gal}(k_z/K)$ act naturally on the group $S_l(k_z^\times) = k_z^\times/(k_z^\times)^l$. In this section, we consider the structure of $S_l(k_z^\times)$ as a Galois module.

Let τ be a fixed generator of $\mathrm{Gal}(k_z/k)$, so $\mathrm{Gal}(k_z/k) = \langle\tau\rangle$ and $\mathrm{Gal}(k_z/K) = \langle\tau^m\rangle$. Let g be a primitive root modulo l such that $\tau(\zeta_l) = \zeta_l^g$. For $1 \leq i \leq l-1$, set

$$e_i(k_z/k) := \frac{1}{l-1} \sum_{1 \leq j \leq l-1} (g^m)^{-ij} \tau^j,$$

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press

and for $1 \le i \le d$, set

$$e_i(k_z/K) := \frac{1}{d} \sum_{1\le j\le d} (g^m)^{-ij} (\tau^m)^j.$$

It is known that the $e_i(k_z/k)$'s (respectively $e_i(k_z/K)$'s) are orthogonal idempotents in the group ring $\mathbb{F}_l[\mathrm{Gal}(k_z/k)]$ (respectively $\mathbb{F}_l[\mathrm{Gal}(k_z/K)]$) over the finite field $\mathbb{F}_l$ of l elements. Therefore,

$$S_l(k_z^\times) = \bigoplus_{1\le i\le l-1} e_i(k_z/k) S_l(k_z^\times).$$

Let S_i^k as the eigenspace corresponding to $e_i(k_z/k)$, that is,

$$S_i^k := e_i(k_z/k) S_l(k_z^\times) = \{e_i(k_z/k)(x) \mid x \in S_l(k_z^\times)\}.$$

Similarly, we define S_i^K by

$$S_i^K := e_i(k_z/K) S_l(k_z^\times) = \{e_i(k_z/K)(x) \mid x \in S_l(k_z^\times)\}.$$

If λ is the self-isogeny on T of degree l inducing the Kummer duality κ_K, then S_1^K and $T(K)/\lambda T(K)$ are closely related to each other.

Proposition 2.1. *Subgroups of S_1^K are in one-to-one correspondence with those of $T(K)/\lambda T(K)$.*

Proof. Since T is an algebraic torus over K, we can construct an isomorphism $\psi : T(\overline{K}) \cong (\overline{K}^\times)^d$ which maps $P \in T(K)$ to $\psi(P) = (\alpha_1, \ldots, \alpha_d)$ for some $\alpha_i \in k_z^\times$.

First, we define a map φ_K from $T(K)/\lambda T(K)$ to S_1^K. Note that if $P \in \lambda T(K)$, then $K(\lambda^{-1}(P)) = K$. So we assume that $P \in T(K)$ does not belong to $\lambda T(K)$. Then, $K(\lambda^{-1}(P))$ is a cyclic extension of K of degree l [3, Theorem 1.1] and $K(\lambda^{-1}(P))(\zeta_l) = k_z(\sqrt[l]{\alpha_1^{e_1}})$ [3, Proposition 6.3], where $\alpha_1^{e_1} = e_1(k_z/k)(\alpha_1)$. Also, we know that if $u = 1$ in S_1^K, then $k_z(\sqrt[l]{u}) = k_z$. Assuming that $u \in S_1^K$ is not the identity, $k_z(\sqrt[l]{u})$ is a cyclic extension of k_z of degree l, and there exists a cyclic extension L of K of degree l such that $L(\zeta_l) = k_z(\sqrt[l]{u})$ [1, Theorem 5.3.5]. On the other hand, it is known that the fields $k_z(\sqrt[l]{u^i})$ $(1 \le i \le l-1)$ are mutually isomorphic by Kummer theory, for $1 \le i \le l-1$. Hence, we can define $\varphi_K(P) = \langle \alpha_1^{e_1} \rangle$ and $K(\lambda^{-1}(P))(\zeta_l) = k_z(\sqrt[l]{\alpha_1^{e_1}})$. It is easy to check that φ_K is a surjective map.

Next, we assume that $\varphi_K(P) = \langle \alpha \rangle$, $\varphi_K(Q) = \langle \beta \rangle$ and $k_z(\sqrt[l]{\alpha}) = k_z(\sqrt[l]{\beta})$ for $P, Q \in T(K) \backslash \lambda T(K)$. Let L_1 (respectively L_2) be a cyclic extension of degree l over K such that $L_1(\zeta_l) = k_z(\sqrt[l]{\alpha})$ (respectively $L_2(\zeta_l) = k_z(\sqrt[l]{\beta})$). Since $k_z(\sqrt[l]{\alpha}) = k_z(\sqrt[l]{\beta})$, we have $L_1 = L_2$. Therefore, $\langle P \rangle = \langle Q \rangle$ in $T(K)/\lambda T(K)$, that is, φ_K is a bijective map. □

For simplicity, in the following discussion, we shall identify an element of S_1^K with the coset of $S_l(k_z^\times)$ which contains the element.

By Proposition 2.1, we may study the structure of S_1^K instead of $T(K)/\lambda T(K)$. Thus, we consider the Galois module structures of $S_l(k_z^\times)$, S_i^k and S_i^K. A basis of $U^{(1)}(k_z)$ as a $\mathbb{Z}_l$-module is given in [2]. Let ξ be a primitive $(l^n - 1)$th root of unity in k.

Proposition 2.2 [2, I(6.4)]. *The $(l-1)n+1$ elements*

$$u_l := 1+\eta\pi^l, \quad u_{i,j} := 1+\xi^i\pi^j \quad (0\le i\le n-1, 1\le j\le l-1)$$

constitute a $\mathbb{Z}_l$-basis of $U^{(1)}(k_z)$. Here, π is a prime element of k_z and $\eta=\xi^i$ for some $i\ge 0$ such that $1+\xi^i\pi^l$ is not an lth power in $U^{(1)}(k_z)$.

The structure of the multiplicative group $k_z^\times$ is given by $k_z^\times \cong \langle\pi\rangle\times\langle\xi\rangle\times U^{(1)}(k_z)$. Noting that $\langle\xi\rangle/(\langle\xi\rangle)^l=1$ since $(l^n-1,l)=1$, we readily get the following proposition.

Proposition 2.3. *If $l=p$, then the $(l-1)n+2$ elements π, u_l and $u_{i,j}$ constitute an $\mathbb{F}_l$-basis of $S_l(k_z^\times)$, where i and j run over $0\le i\le n-1$ and $1\le j\le l-1$.*

In the following, we fix a prime element $\pi=\zeta_l-1$ and we consider the action of $\tau\in\mathrm{Gal}(k_z/K)$ on $S_l(k_z^\times)$.

Lemma 2.4. *The matrix X of τ with respect to the basis $(\pi, u_l, u_{n-1,l-1}, u_{n-2,l-1},\dots,u_{0,1})$ is given by*

$$X=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0\\ * & g^l & * & \cdots & *\\ * & 0 & A_{l-1} & \ddots & \vdots\\ \vdots & \vdots & \ddots & \ddots & *\\ * & 0 & \cdots & 0 & A_1\end{pmatrix}.$$

Here, for $1\le j\le l-1$, the A_j are the $n\times n$ matrices

$$A_j=\begin{pmatrix} g^j & 0 & \cdots & 0 & 0\\ 0 & g^j & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & g^j & 0\\ 0 & 0 & \cdots & 0 & g^j\end{pmatrix}.$$

Proof. To avoid heavy notation, we rename the basis in the statement of the lemma as $(v_1,\dots,v_{n(l-1)+2})=(\pi,u_l,u_{n-1,l-1},\dots,u_{0,1})$ so that $u_{i,j}=v_{(l-j)n+2-i}$. We set $X=(x_{st})$. First, we show that the first column is 0 except for x_{11}. Recall that g is the chosen primitive root satisfying $\tau(\zeta_l)=\zeta_l^g$. Define

$$\omega := \frac{\zeta_l^g-1}{\zeta_l-1}=\zeta_l^{g-1}+\cdots+\zeta_l+1,$$

so that $\tau(\pi)=\omega\pi$. Since ω is a unit element, $v_{k_z}(\tau(\pi))=1$. Moreover, $v_{k_z}(\tau(v_i))=0$ for all $i\ge 2$ because

$$\tau(v_2)=\tau(1+\eta\pi^l)=1+\eta(\omega\pi)^l$$

and

$$\tau(v_i)=\tau(u_{a,b})=\tau(1+\xi^a\pi^b)=1+\xi^a(\omega\pi)^b$$

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press

for all $i \geq 3$ and some a and b. Hence the entries in the first column of X are $x_{11} = 1$ and $x_{1t} = 0$ for all $t \geq 2$.

Next we show that the A_j are diagonal matrices whose diagonal entries are integer powers of g. Since $\omega \equiv g \pmod{\pi}$ and $\tau(\xi) = \xi$,

$$\tau(u_{i,j}) \equiv 1 + \xi^i \omega^j \pi^j \equiv 1 + g^j \xi^i \pi^j \equiv (1 + \xi^i \pi^j)^{g^j} \pmod{\pi^{j+1}}$$

for each j. Hence, $\tau(u_{i,j}) \equiv {u_{i,j}}^{g^j} \pmod{\pi^{j+1}}$. Since the ξ^i are independent, the A_j are diagonal matrices. In a similar way, we can prove the assertion for $\tau(u_l)$.

Finally, we show that $x_{st} = 0$ for any $s > 2$ and $s > t$. To do this, pick out the jth column of X as $(x_1, \dots, x_{(l-1)n+2})$ and consider the action of τ on the jth basis vector v_j for $j > 1$. We claim that $x_{j'} = 0$ for all $j' > j$. Set $v_j = u_{a,b}$ and write $\tau(v_j)$ as

$$\tau(v_j) = \prod_{2 \leq i \leq (l-1)n+2} v_i^{x_i} \quad \text{in } S_l(k_z^\times). \tag{2.1}$$

Let i' be the maximal number i such that $x_i \neq 0$. Then, the right-hand side of (2.1) is

$$\prod_{2 \leq i \leq (l-1)n+2} v_i^{x_i} = \prod_{2 \leq i \leq i'} v_i^{x_i}.$$

If $v_{i'} = u_{a',b'}$, then

$$v_{k_z}\Big(\prod_{2 \leq i \leq i'} v_i^{x_i} - 1\Big) = b',$$

and the left-hand side of (2.1) satisfies

$$v_{k_z}(\tau(v_j) - 1) = v_{k_z}(\tau(\zeta^a \pi^b)) = a \cdot v_{k_z}(\zeta) + b \cdot v_{k_z}(\omega) + b \cdot v_{k_z}(\pi) = b.$$

Thus, $b' = b$. Moreover, since $\tau(v_j) \equiv {v_j}^{g^m} \pmod{\pi^{m+1}}$ for some $m \geq 0$, we have $a' = a$. Hence, we have shown that $i' = j$ and $x_{j'} = 0$ for all $j' > j$. □

Lemma 2.4 gives a formula for the dimension of S_i^k for $1 \leq i \leq l-1$.

Proposition 2.5. *For each i with $1 \leq i \leq l-1$,*

$$\dim_{\mathbb{F}_l} S_i^k = \begin{cases} n+1 & \text{for } i = 1 \text{ or } l-1, \\ n & \text{for } 1 < i < l-1. \end{cases}$$

Proof. Let X be the matrix defined in Lemma 2.4. Its characteristic polynomial is

$$(x-1)(x-g^l)(x-g^{l-1})^n \cdots (x-g)^n = (x-1)^{n+1}(x-g)^{n+1}(x-g^2)^n \cdots (x-g^{l-2})^n$$

and its minimal polynomial is

$$(x-1)(x-g)\cdots(x-g^{l-2}).$$

Since this polynomial has no multiple roots, the matrix X is diagonalisable and the dimension of each eigenspace S_i^k coincides with the multiplicity of the corresponding eigenvalue g^i. □

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press

Moreover, we can give the relationship between S_i^k and S_i^K.

LEMMA 2.6. *For* $1 \leq i \leq d$,

$$S_i^K = \bigoplus_{\substack{1\leq j<l-1 \\ j\equiv i \pmod d}} S_j^k.$$

PROOF. For $u \in S_j^k$, we have $\tau^m(u) = g^{mj}u$ since $\tau(u) = g^j u$. Furthermore, any element $u' \in S_{j+d}^k$ satisfies

$$\tau^m(u') = g^{m(j+d)}u' \equiv g^{mj}u' \pmod l.$$

Thus, $S_i^K \supset S_{j'}^k$ for any $j' \equiv i \pmod d$ and

$$S_i^K \supset \bigoplus_{\substack{1\leq j<l-1 \\ j\equiv i \pmod d}} S_j^k.$$

However, we know

$$\bigoplus_{1\leq i\leq d} S_i^K = S_l(k_z^\times)$$

and

$$\bigoplus_{1\leq i\leq d}\Big(\bigoplus_{\substack{1\leq j\leq l-1 \\ j\equiv i \pmod d}} S_j^k\Big) = \bigoplus_{1\leq j\leq l-1} S_j^k = S_l(k_z^\times)$$

and the assertion follows. □

From this, we derive the dimension of S_i^K for $1 \leq i \leq l-1$.

PROPOSITION 2.7. *For* $1 \leq i \leq d$,

$$\dim_{\mathbb{F}_l} S_i^K = \begin{cases} mn+1 & \text{for } i = 1 \text{ or } d, \\ mn & \text{for } 1 < i < d. \end{cases}$$

Finally, we determine the basis of S_1^K using Proposition 2.3 and Lemma 2.6.

THEOREM 2.8. *Keep the above notations. The $mn+1$ elements $u_{i,j}$ and u_l constitute an $\mathbb{F}_l$-basis of S_1^K, where i and j run over $0 \leq i \leq n-1$ and $1 \leq j \leq l-1$ and $j \equiv 1 \pmod d$.*

3. Proof of the main theorem

Let us recall the setting in Section 1. We have assumed that there exists a self-isogeny λ on $T = R_{k_z/K}\mathbb{G}_m$ of degree l whose kernel is contained in the group $T(K)$ of K-rational points. Let P be a K-rational point on the torus T. Then we have a cyclic extension $L = K(\lambda^{-1}(P))$ over K. In this section, we determine the ramification in L/K using the structure of S_1^K. To do this, first we describe the ramification in the Kummer extension L_z/k_z using Hecke's theorem which we recall now.

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press

PROPOSITION 3.1 [1, Theorem 10.2.9]. *Let π be a prime element in k_z and $L_z = k_z(\sqrt[l]{\alpha})$ with $\alpha \in S_1^K - \{1\}$. Let $d(L_z/k_z)$ be the discriminant of L_z/k_z. Let a be the largest exponent w such that the congruence*

$$x^l \equiv \alpha \pmod{\pi^{w+v_{k_z}(\alpha)}}$$

has a solution. Then

(1) *l is unramified in L_z/k_z if and only if $a = l$;*
(2) *l is totally ramified in L_z/k_z if and only if $a \le l-1$ and in that case $v_{k_z}(d(L_z/k_z)) = (l-1)(l+1-a)$.*

Let $\widehat{T} = \mathrm{Hom}(T, \mathbb{G}_{m,k_z})$ be the group of characters of T and, for each $i \ge 1$, set $T^{(i)}(K) = \mathrm{Hom}_{\mathrm{Gal}(k_z/K)}(\widehat{T}, U^{(i)}(k_z))$ (see [5, Section 2]), where the $U^{(i)}(k_z)$ are the groups of higher principal units defined by (1.2). Note that the $T^{(i)}(K)$'s are subgroups of $\mathrm{Hom}_{\mathrm{Gal}(k_z/K)}(\widehat{T}, U(k_z))$, which is the maximal compact subgroup of $T(K)$.

Now we shall prove the main theorem.

THEOREM 3.2. *Let $p = l$ be an odd prime. Let K be a finite extension of k of degree m and set $d = (l-1)/m$. If $P \in T^{(jd+1)}(K)$ and $P \notin T^{(jd+2)}(K)$ for some $0 \le j \le m$, then the conductor $\mathfrak{f}$ of the cyclic extension $K(\lambda^{-1}(P))/K$ satisfies*

$$v_K(\mathfrak{f}) = \begin{cases} m - j + 1 & \text{for } 0 \le j < m, \\ 0 & \text{for } j = m. \end{cases}$$

In particular, $K(\lambda^{-1}(P))/K$ is an unramified extension if and only if $P \in T^{(l)}(K)$.

PROOF. We denote the discriminant of L/K by $d(L/K)$. Since k_z and L are intermediate fields of L_z/K,

$$\mathcal{N}_{L_z/K} = \mathcal{N}_{k_z/K} \circ \mathcal{N}_{L_z/k_z} = \mathcal{N}_{L/K} \circ \mathcal{N}_{L_z/L},$$

by the chain rule for the norm map. Using this equation,

$$\mathcal{N}_{k_z/K}(d(L_z/k_z)) \cdot d(k_z/K)^l = \mathcal{N}_{L/K}(d(L_z/L)) \cdot d(L/K)^d.$$

If $P \in T^{(jd+1)}(K)$ and $P \notin T^{(jd+2)}(K)$ for some $0 \le j < m$, then, by Proposition 3.1(2), $v_{k_z}(d(L_z/k_z)) = (l-1)(l-jd)$. Now $v_K(\mathcal{N}_{k_z/K}(d(L_z/k_z)))$ equals $(l-1)(l-jd)$ since k_z/K is a totally ramified extension. Since k_z/K is a tamely ramified extension and L_z/L is a tamely and totally ramified extension, $v_K(d(k_z/K)^l) = l(d-1)$ and $v_K(\mathcal{N}_{L/K}(d(L_z/L))) = d-1$. Since $d(L/K) = \mathfrak{f}^{l-1}$,

$$(l-1)(l-jd) + l(d-1) = (d-1) + (l-1)d v_K(\mathfrak{f}).$$

Therefore, we have shown that $v_K(\mathfrak{f}) = m - j + 1$.

For the case $j = m$, we have $v_K(\mathfrak{f}) = 0$ since L/K is an unramified extension by Proposition 3.1(1). □

In Theorem 3.2, we calculated the conductor of $K(\lambda^{-1}(P))/K$ when $P \in T^{(jd+1)}(K)$ and $P \notin T^{(jd+2)}(K)$ for some j with $0 \le j \le m$. By counting the number of such points P, we can calculate the number of cyclic extensions of K of degree l with a fixed conductor.

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press

THEOREM 3.3. *Let $p = l$ be an odd prime. For $0 \le j < m$, the number of cyclic extensions of $K \subset \overline{\mathbb{Q}}_l$ of degree l whose conductor $\mathfrak{f}$ satisfies $v_K(\mathfrak{f}) = m - j + 1$ is $l^{(m-(j+1))n+1}(l^n - 1)/(l - 1)$ up to isomorphism in $\overline{\mathbb{Q}}_l$.*

PROOF. Let r_j be the number of $u \in S_1^K$ such that $u \in U^{(jd+1)}(k_z)$ and $u \notin U^{(jd+2)}(k_z)$. Write

$$u = u_l^{a_l} \prod_{\substack{0 \le i \le n-1 \\ 1 \le j \le l-1 \\ j \equiv 1 \pmod{d}}} u_{i,j}^{a_{i,j}}$$

with $0 \le a_{i,j}, a_l \le l - 1$. If $0 \le j < m$, then $a_{i,j'} = 0$ for $0 \le j' < j$ since $v_{k_z}(u - 1) = jd + 1$. Since at least one of $a_{0,jd+1}, \ldots, a_{n-1,jd+1}$ is nonzero,

$$r_j = l^{(mn+1)-n-jn} \cdot (l^n - 1) = l^{(m-(j+1))n+1} \cdot (l^n - 1).$$

On the other hand, it is known that the fields $k_z(\sqrt[l]{u^i})$ $(1 \le i \le l - 1)$ are mutually isomorphic by Kummer theory. By Proposition 2.1, a cyclic extension of k_z of degree l corresponds to a cyclic extension of K of degree l. So we can calculate the number of cyclic extensions L/K by dividing r_j by $l - 1$. □

REMARK 3.4. In Theorem 3.3, we calculated the number of cyclic extensions of $K \subset \overline{\mathbb{Q}}_l$ of degree l with a fixed conductor, assuming that there exists an isogeny λ on T of degree l whose kernel is contained in $T(K)$. If there exists no such λ, then there seems to be no known method of counting these extensions.

Theorems 3.2 and 3.3 deal only with the case of $p = l$. Finally, we briefly mention the case $l \nmid p^n - 1$ and $p \ne l$. Let k be an unramified extension of $\mathbb{Q}_p$ of degree n and $q = p^n$. Keep the above notation.

Since $(l, q - 1) = 1$, we see that k_z/k is an unramified extension. The map $u \mapsto u^l$ is an isomorphism since $v_{k_z}(l) = 0$. Thus, $(U^{(1)}(k_z))^l = U^{(1)}(k_z)$. Hence, we have proved the following result.

PROPOSITION 3.5. *If $l \nmid q - 1$ and $l \ne p$, then the 2 elements p, ζ_{q-1} constitute an $\mathbb{F}_l$-basis of S_1^K.*

Let τ be a generator of $\mathrm{Gal}(k_z/k)$. Then, τ acts trivially on both p and ζ_{q-1}. Thus, $S_1^K = S_l(k_z^\times)$ for any intermediate field K of k_z/k. Consequently, we obtain the following proposition.

PROPOSITION 3.6. *Let p be an odd prime and l a prime satisfying $l \nmid q - 1$ and $p \ne l$. Set $T(U(k_z)) = \mathrm{Hom}_{\mathrm{Gal}(k_z/K)}(\widehat{T}, U(k_z))$. Then, for $P \in T(K)$ with $P \notin \lambda T(K)$, $K(\lambda^{-1}(P))/K$ is a tamely ramified extension if and only if $P \notin T(U(k_z))$; in that case the conductor $\mathfrak{f}$ satisfies $v_K(\mathfrak{f}) = 1$.*

Acknowledgement

The author would like to thank the referee for many helpful comments and careful reading of the manuscript.

References

[1] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, 193 (Springer, New York, 2000).

[2] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions*, 2nd edn, Translations of Mathematical Monographs, 121 (American Mathematical Society, Providence, RI, 2002).

[3] M. Kida, 'Descent Kummer theory via Weil restriction of multiplicative groups', *J. Number Theory* **130**(3) (2010), 639–659.

[4] T. Komatsu, 'Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory', *Manuscripta Math.* **114**(3) (2004), 265–279.

[5] T. Ono, 'Arithmetic of algebraic tori', *Ann. of Math. (2)* **74** (1961), 101–139.

MASAMITSU SHIMAKURA, Department of Mathematics,
Tokyo University of Science, 1-3, Kagurazaka, Shinjuku,
Tokyo, 162-8601, Japan
e-mail: 1115704@ed.tus.ac.jp

https://doi.org/10.1017/S0004972717000491 Published online by Cambridge University Press