JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Masanari KIDA

On metacyclic extensions

Tome 24, n° 2 (2012), p. 339-353.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_2_339_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 339-353

On metacyclic extensions

par Masanari KIDA

Résumé. Nous construisons des extensions galoisiennes de groupes de Galois métacycliques variés au moyen d'une théorie de Kummer émanant d'une isogénie de certains tores algébriques. En particulier, notre méthode nous permet de construire des tores algébriques paramétrant des extensions métacycliques.

Abstract. Galois extensions with various metacyclic Galois groups are constructed by means of a Kummer theory arising from an isogeny of certain algebraic tori. In particular, our method enables us to construct algebraic tori parameterizing metacyclic extensions.

1. Introduction

A finite group G is called metacyclic if it contains a normal cyclic subgroup N such that the quotient group G/N is also cyclic. The category of metacyclic groups contains important families of groups such as dihedral groups and Frobenius groups. A Galois extension L/k is called a metacyclic extension if the Galois group $\mathrm{Gal}(L/k)$ is isomorphic to a metacyclic group. In this paper, we give a method to construct metacyclic extensions using a Kummer theory without roots of unity studied in our previous paper [10]. Évariste Galois already knew that if a polynomial of prime degree $\ell(\geq 5)$ is solvable, then the Galois group of the polynomial is a Frobenius group (see [7, Lemma 7.1.2]). Thus our method enables us to construct such solvable extensions. In their paper [14], Nakano and Sase also study a construction of metacyclic extensions, which is a generalization of a former result of Imaoka and Kishi [6] on Frobenius and dihedral extensions. Our construction supersedes their construction in some respect. Furthermore, because our construction comes from a Kummer theory and there are geometric objects parameterizing the field extensions, we can expect to get more algebraic and arithmetic information about the extensions.

After we give some preliminaries on metacyclic groups and the Kummer theory in the next section, we state and prove one of our main theorem in Section 3. In Section 4, we explain geometry behind our construction. In

Manuscrit reçu le 26 janvier 2011.
This research is supported in part by Grant-in-Aid for Scientific Research (C) (No. 19540015), Ministry of Education, Science, Sports and Culture, Japan.

fact, we show that our metacyclic extensions are parameterized by rational points on certain algebraic tori defined over the base field. In Section 5, we give a relationship between our construction and the construction due to Sase and Nakano. Several examples are given in the final section.

Notation. The following symbols are used throughout this paper. Let ℓ be an odd prime number fixed once for all. We denote a field of ℓ elements by $\mathbb{F}_\ell$. We also fix a base field k whose characteristic is different from ℓ. We assume that any separable extensions of k are contained in a fixed separable closure k_{sep} of k. For an integer m prime to the characteristic of k, we denote by ζ_m a primitive m-th root of unity in k_{sep}. For any separable extension K over k, we write K_c for the ℓ-th cyclotomic extension $K(\zeta_\ell)$.

Let r be a divisor of $\ell - 1$ and F a cyclic extension over k of degree r

$$r = [F : k].$$

We denote by σ a generator of the Galois group of F/k:

$$\mathrm{Gal}(F/k) = \langle \sigma \rangle.$$

Let n be the degree of the cyclotomic extension F_c/F:

$$n = [F_c : F];$$

and τ a generator of the Galois group of F_c/F:

$$\mathrm{Gal}(F_c/F) = \langle \tau \rangle.$$

Since both k_c/k and F/k are abelian extensions, $F_c = Fk_c$ is also an abelian extension over k of degree nr. Therefore there exists a subgroup of $\mathrm{Gal}(F_c/k)$ isomorphic to $\mathrm{Gal}(F/k)$ whose generator is a lift of σ. We denote the generator also by σ. Then we have an isomorphism

$$\mathrm{Gal}(F_c/k) \cong \langle \sigma \rangle \times \langle \tau \rangle.$$

For a finite group G, a field extension L/k is called a G-extension if it is a Galois extension whose Galois group is isomorphic to G.

Other notation will be introduced when we need it.

2. Preliminaries

In this section, we give some preliminaries from group theory and a Kummer theory for certain algebraic tori.

2.1. Metacyclic groups. We refer to [3, Section 47] for basic facts on metacyclic groups. A metacyclic group G is an extension of a cyclic group with cyclic kernel N:

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1 \text{ (exact)}$$

In this paper, we are solely concerned with the case where the order of N is a prime number ℓ. We write $N = \langle \rho \rangle$ and $G/N = \langle \sigma N \rangle$. Since N is normal

in G, we can find an element x in $\mathbb{F}_\ell^\times$ such that $\sigma^{-1}\rho\sigma = \rho^x$ holds. For a positive integer m, we have $\sigma^{-m}\rho\sigma^m = \rho^{x^m}$. Let s be the order of x in $\mathbb{F}_\ell^\times$ and r the order of σN. Then it follows that

$$s \mid r \mid \ell - 1. \tag{2.1}$$

Hence the extension splits by a theorem of Schur [4, Theorem 15.2.2] and there exists a subgroup H of G isomorphic to G/N satisfying $G = N \rtimes H$. Note that if x and x' generate the same subgroup in $\mathbb{F}_\ell^\times$, then the corresponding metacyclic groups are isomorphic. Therefore such a group is determined by ℓ, r and s and thus we denote this group by $M_\ell(r,s)$:

$$M_\ell(r,s) = \langle \sigma, \rho \mid \sigma^r = 1, \rho^\ell = 1, \sigma^{-1}\rho\sigma = \rho^x, \mathrm{ord}(x \bmod \ell) = s \rangle.$$

It is easy to observe that

$$M_\ell(r,s) \text{ is abelian } \iff s = 1;$$
$$M_\ell(r,s) \text{ is a Frobenius group } F_{\ell r} \iff s = r;$$
$$M_\ell(r,s) \text{ is a dihedral group } D_\ell \text{ of order } 2\ell \iff s = r = 2.$$

2.2. Kummer theory via algebraic tori. Suppose that there exists an integer-coefficient polynomial

$$\mathscr{P}(t) = c_1 + c_2 t + \cdots + c_n t^{n-1} \in \mathbb{Z}[t] \tag{2.2}$$

of degree $n-1$ satisfying the following two conditions:

$$\mathbb{Z}[\zeta_n]/(\mathscr{P}(\zeta_n)) \cong \mathbb{Z}/(\ell) = \mathbb{F}_\ell; \tag{2.3}$$

and

$$\mathscr{P}(\zeta_n^i) \in \mathbb{Z}[\zeta_n^i]^\times \text{ for all } i \text{ with } (n,i) > 1. \tag{2.4}$$

We assume that the ring isomorphism (2.3) induces a group isomorphism

$$\nu_k \ : \ \mathrm{Gal}(k_c/k) \xrightarrow{\sim} \langle \zeta_n \bmod \ \mathscr{P}(\zeta_n) \rangle. \tag{2.5}$$

Therefore we have $n = [k_c : k]$. Let $R_{k_c/k}\mathbb{G}_m$ be the Weil restriction of scalars of the multiplicative group. The algebraic torus $R_{k_c/k}\mathbb{G}_m$ is an n-dimensional torus defined over k splitting over k_c. For other basic properties of $R_{k_c/k}\mathbb{G}_m$, see [15, 3.12]. Then the circulant matrix

$$\mathrm{circ}(c_1, c_2, \ldots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix} \tag{2.6}$$

defines an endomorphism Λ of degree ℓ on the character module $\widehat{R_{F_c/k}\mathbb{G}_m}$ of $R_{k_c/k}\mathbb{G}_m$, which is, by definition,

$$\widehat{R_{F_c/k}\mathbb{G}_m} = \mathrm{Hom}_{k\text{-schemes}}(R_{k_c/k}\mathbb{G}_m, \mathbb{G}_{m,k}).$$

In fact, we can show that $|\det(\mathrm{circ}(c_1, c_2, \ldots, c_n))| = \ell$ under our assumptions. In the dual category, we have a self-isogeny λ of degree ℓ on the k-torus $R_{k_c/k}\mathbb{G}_m$. The following theorem is proved in [10].

Theorem 2.1. *Let λ be the self-isogeny of $R_{k_c/k}\mathbb{G}_m$ of degree ℓ defined as above. Then every point in the kernel of λ is k-rational and the exact sequence attached to the isogeny λ*

$$1 \longrightarrow \ker\lambda \longrightarrow R_{k_c/k}\mathbb{G}_m \xrightarrow{\lambda} R_{k_c/k}\mathbb{G}_m \longrightarrow 1 \quad \textit{(exact)}$$

induces the Kummer duality

$$\kappa_k \ : \ R_{k_c/k}\mathbb{G}_m(k)/\lambda R_{k_c/k}\mathbb{G}_m(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k_{\mathrm{sep}}/k), \ker\lambda(k)). \tag{2.7}$$

For any $P \in R_{k_c/k}\mathbb{G}_m(k)$, the image $\kappa_k(P)$ is a homomorphism χ_P sending every $s \in \mathrm{Gal}(k_{\mathrm{sep}}/k)$ to P^{1-s}. As a consequence, every cyclic extension over k of degree ℓ is obtained by adjoining an inverse image $\lambda^{-1}(P)$ of some $P \in R_{k_c/k}\mathbb{G}_m(k)$ and a generator ρ of $\mathrm{Gal}(k(\lambda^{-1}(P))/k)$ acts by $\rho(\lambda^{-1}(P)) = Z\lambda^{-1}(P)$ with some $Z \in \ker\lambda(k)$.

It is known that this Kummer theory holds for the following cases:

- If n is a prime and if there exists an element $\lambda \in \mathbb{Z}[\zeta_n]$ whose norm is ℓ. Then we can find $\mathscr{P}(t)$ satisfying our assumptions.
- We can always construct $\mathscr{P}(t)$ in the case where $n = 4$.
- The base field k of the Kummer theory can be descended to the field $\mathbb{Q}$ of rational numbers when $\ell = 3, 5, 7,$ and 11.

See [10, Section 4] for the detail.

3. Algebraic theorem

A field extension L/k is called metacyclic extension if it is a Galois extension whose Galois group is isomorphic to a metacyclic group. Our aim is constructing *all* metacyclic extensions with Galois group $M_\ell(r, s)$ over k containing a given intermediate field F under certain assumptions. We sometimes refer to such an extension by $L/F/k$. Here we understand that F is the fixed field by the normal subgroup of order ℓ in $M_\ell(r, s)$.

From now on, suppose that we are given a cyclic extension F/k of degree r satisfying the following assumption. The first assumption is that there exists a Kummer theory κ_k by an n-dimensional algebraic torus $R_{k_c/k}\mathbb{G}_m$ explained in Section 2.2. The second assumption is $F \cap k_c = k$. Then κ_k naturally lifts to

$$\kappa_k \times F \ : \ R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k_{\mathrm{sep}}/F), \ker\lambda(k)). \tag{3.1}$$

Hence every cyclic extension of F can be obtained by this isomorphism. On the other hand, the Galois group $\mathrm{Gal}(F/k) = \langle\sigma\rangle$ naturally acts on the left hand side of this isomorphism. We use the isomorphism (3.1) and the

Galois action to construct metacyclic extensions L over k that are cyclic over F.

By (3.1), the quotient group $R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)$ is a vector space over $\mathbb{F}_\ell$. Therefore the group ring $\mathbb{F}_\ell[\sigma]$ acts on this quotient. Let χ be a character of $\mathrm{Gal}(F/k)$

$$\chi \ : \ \mathrm{Gal}(F/k) \longrightarrow \mathbb{F}_\ell^\times$$

sending σ to an element of $\mathbb{F}_\ell$ of order r. Then

$$e_j = \frac{1}{r}\sum_{i=0}^{r-1} \chi^j(\sigma^{-i})\sigma^i \in \mathbb{F}_\ell[\sigma] \tag{3.2}$$

are orthogonal idempotents ($j = 0, 1, \ldots, r-1$) in $\mathbb{F}_\ell[\sigma]$.

Now we can state the algebraic side of our result.

Theorem 3.1. *Let F be a cyclic extension of a field k with Kummer theory κ_k (2.7) of degree r such that $F \cap k_c = k$. For each $j = 0, 1, \ldots, r-1$, the image of $e_j\left(R_{F_c/F}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right)$ under $\kappa_k \times F$ corresponds to metacyclic extensions over k with Galois group isomorphic to $M_\ell(r, s)$ where $s = r/(j, r)$. In particular, it corresponds to abelian extensions if $j = 0$ and to Frobenius extensions if $(j, r) = 1$.*

Conversely, every $M_\ell(r, s)$-extension over k containing F arises in this way.

Proof. Let P be an F-rational point of $R_{k_c/k}\mathbb{G}_m$ whose class $\overline{P}$ is an element of $\mathscr{E}_j = e_j\left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right)$. We assume that $\overline{P}$ is non-trivial. Then by Theorem 2.1 the extension $L = F(\lambda^{-1}(P))$ is a cyclic extension over F of degree ℓ. We first show that L is a Galois extension over k. Let $\tilde{\sigma}$ be an extension of σ to L. If we write $Q = \lambda^{-1}(P)$, then we have

$$\lambda(\tilde{\sigma}(Q)) = \tilde{\sigma}(\lambda(Q)) = \tilde{\sigma}(P) = \sigma(P)$$

because the isogeny λ is defined over k. This shows that $F(\tilde{\sigma}(Q)) = F(\lambda^{-1}(\sigma P))$. On the other hand, since $\overline{P}$ belongs to $\mathscr{E}_j$, we have $\sigma\overline{P} = \overline{P}^{\chi(\sigma)^j}$ where $u = \chi(\sigma)^j$ is an element of $\mathbb{F}_\ell$ of order s. Since u is invertible modulo ℓ, $\overline{P}$ and $\overline{P}^u$ generate the same subgroup in $\mathscr{E}_j$. By Kummer theory, this implies $F(\tilde{\sigma}(Q)) = F(Q)$. Thus it yields $k(\tilde{\sigma}(Q)) = k(Q)$ as we desired.

The Galois group $\mathrm{Gal}(L/k)$ fits in the following exact sequence:

$$1 \longrightarrow \mathrm{Gal}(L/F) \longrightarrow \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(F/k) \longrightarrow 1 \ \text{(exact)}.$$

Since the orders of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(F/k)$ are relatively prime, the exact sequence splits. Let ρ be a generator of $\mathrm{Gal}(L/F)$. Let us denote a unique lift of σ to $\mathrm{Gal}(F/k)$ by the same symbol. Then it remains to show that σ and ρ satisfy the relation $\sigma^{-1}\rho\sigma = \rho^u$. We resume the previous calculation:

$$\lambda(\sigma(Q)) = \sigma(P) = P^u = \lambda(Q^u)$$

in $\mathscr{E}_j$. Let Z be an element in $\ker\lambda(k_{\mathrm{sep}}) = \ker\lambda(k)$ such that $\rho(Q) = QZ$. Since the order of ρ is ℓ, the order of Z is also ℓ. From the above calculation, it follows that $\sigma(Q) = Q^u R$ with some $R \in R_{k_c/k}\mathbb{G}_m(F)$. Moreover, since Z is k-rational, we see that $\sigma(Z) = Z$ and $\rho(Z) = Z$ hold. Combining these actions, we obtain

$$\sigma\rho^u(Q) = \sigma(QZ^u) = \sigma(Q)\sigma(Z)^u = Q^u R Z^u$$

and

$$\rho\sigma(Q) = \rho(Q^u R) = \rho(Q)^u \rho(R) = Q^u R Z^u.$$

From this it follows $\sigma^{-1}\rho\sigma = \rho^u$.

Conversely, let $L/F/k$ be any $M_\ell(r,s)$-extension. Since L/F is a cyclic extension, we can write $L = F(\lambda^{-1}(P))$ with some $P \in R_{F_c/F}\mathbb{G}_m(F)$. We have to show that the class $\overline{P}$ of P belongs to $\mathscr{E}_j$ for some j. Since L/k is a Galois extension, for any lift $\tilde{\sigma}$ of σ, we have $k(\tilde{\sigma}(\lambda^{-1}(P))) = k(\lambda^{-1}(P))$. As we saw in the above, $\tilde{\sigma}(\lambda^{-1}(P)) = \lambda^{-1}(\sigma P)$ holds. Therefore we obtain $F(\lambda^{-1}(\sigma P)) = F(\lambda^{-1}(P))$. By Kummer theory, σP and P must generate the same subgroup in the quotient. Hence there exists an integer u satisfying $\sigma P = P^u$ in the quotient. Taking an integer j such that $u \equiv \chi^j(\sigma) \pmod{\ell}$, we conclude $\overline{P} \in \mathscr{E}_j$.

This completes the proof of our theorem. □

Theorem 3.1 shows that, if F satisfies appropriate conditions, we can always dig it to construct metacyclic extensions.

Remark 3.2. We can show a similar theorem for $F = \mathbb{Q}(\zeta_\ell)$ and $k = \mathbb{Q}$. For general ℓ, we do not have a Kummer theory over the base field $\mathbb{Q}$ contrary to our assumption in Theorem 2.1. But we use the classical Kummer theory to prove the theorem in this situation. Note that we have to take account of the action of σ on $Z \in \ker\lambda(F)$ and the resulting s is shifted by this effect (see [2, Theorem 5.3.5]).

Some remarks on a base change and an extension are in order.

Let $L/F/k$ be an $M_\ell(r,s)$-extension and k' an intermediate field in F/k with $[F : k'] = r'$. It is easy to observe that the extension $L/F/k'$ is also a metacyclic extension and the Galois group is isomorphic to $M_\ell\left(r', \frac{s}{(s,r/r')}\right)$. We write $e_j(F/k)$ for e_j defined by (3.2) and $e_j(F/k')$ for the corresponding object for the extension F/k'.

We have the following lemma.

Lemma 3.3. *Let $t = [k' : k]$. We have*

$$e_j(F/k') = \sum_{i=0}^{t-1} e_{j+r'i}(F/k).$$

If the $e_{j+r'i}(F/k)$-component parametrizes $M_\ell(r,s)$-extensions, then the $e_j(F/k')$-component parametrizes $M_\ell\left(r', \frac{s}{(s,r/r')}\right)$-extensions.

The first half can be shown by a standard calculation with characters. For the latter half, we have $s =$ the order of $\zeta_r^j = r/(r,j)$. Then we can show that the order of $\zeta_{r'}^{j'}$ is $s/(s,t)$ by an elementary argument. We omit the detail of the proof.

Since we assume $k_c \cap F = k$, we have $R_{k_c/k}\mathbb{G}_m \times_k k' = R_{k'_c/k'}\mathbb{G}_m$ and there is a map from $R_{k_c/k}\mathbb{G}_m$ to $R_{k'_c/k'}\mathbb{G}_m$. By the above lemma, a natural inclusion map

$$e_{j+r'i}(F/k)\left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right) \longrightarrow e_j(F/k')\left(R_{k'_c/k'}\mathbb{G}_m(F)/\lambda R_{k'_c/k'}\mathbb{G}_m(F)\right)$$

is induced. This map corresponds to the base change k'/k.

Next we consider the following situation. Let $L'/F'/k$ be a metacyclic extension with group $M_\ell(r',s)$ constructed by the Kummer theory $\kappa_{F'}$. Let F be a cyclic extension of k containing F' whose degree $[F:k] = r$ divides $\ell - 1$. Assume that $\kappa_{F'}$ induces a Kummer theory κ_F over F. We use the same symbol λ for the isogeny inducing κ_F. Then the composite field $L = L'F$ is a Galois extension over k. In fact, $L/F/k$ is a metacyclic extension and the Galois group is isomorphic to $M_\ell(r,s)$. This follows from the following lemma.

Lemma 3.4. *We have a natural inclusion*

$$e_j(F'/k)\left(R_{k_c/k}\mathbb{G}_m(F')/\lambda R_{k_c/k}\mathbb{G}_m(F')\right) \longrightarrow e_{[F:F']j}(F/k)\left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right).$$

If the $e_j(F'/k)$-component parametrizes $M_\ell(r',s)$-extensions, then the $e_{[F:F']j}(F/k)$-component parametrizes $M_\ell(r,s)$-extensions.

Proof. First note that there is a natural map $R_{k_c/k}\mathbb{G}_m(F') \longrightarrow R_{k_c/k}\mathbb{G}_m(F)$ induced by inclusion $F' \subset F$.

Let $\mathrm{Gal}(F/k) = \langle\sigma\rangle$ as before. Then we have $\mathrm{Gal}(F'/k) = \langle\sigma\rangle/\langle\sigma^{r'}\rangle$. Let $t = [F:F']$. Then the character group of $\mathrm{Gal}(F'/k)$ is generated by χ^t. Thus

$$e_j(F'/k) = \frac{1}{r'}\sum_{i=0}^{r'-1}\chi^{tj}(\sigma^{-i})\sigma^i$$

is well-defined. Now we compute

$$\begin{aligned} e_{tj}(F/k) &= \frac{1}{r}\sum_{k=0}^{t-1}\sum_{m=0}^{r'-1}\chi^{tj}(\sigma^{-(kr'+m)})\sigma^{kr'+m} \\ &= \frac{1}{r}\sum_{k=0}^{t-1}\sum_{m=0}^{r'-1}\chi^{tj}(\sigma^{-m})\sigma^{kr'+m} \\ &= \frac{1}{r}\left(\sum_{m=0}^{r'-1}\chi^{tj}(\sigma^{-m})\sigma^{m}\right)\sum_{k=0}^{t-1}\sigma^{kr'} \\ &= \frac{1}{t}\mathrm{Tr}_{F/F'}e_j(F'/k), \end{aligned}$$

where $\mathrm{Tr}_{F/F'}$ is the trace map from F to F'. Since $\mathrm{Tr}_{F/F'}$ acts on F' by the multiplication-by-t map, $e_{tj}(F/k)$ acts as $e_j(F'/k)$. This shows the first half of the lemma and the latter half is proved by an elementary calculation. □

The inclusion map in Lemma 3.4 corresponds to the extension F/F'.

4. Geometric counterpart

In this section we construct algebraic tori defined over k parameterizing $M_\ell(r,s)$-extensions over k. This reveals the geometric nature of our construction.

We consider the character module $\widehat{R_{F_c/k}\mathbb{G}_m}$ of $R_{F_c/k}\mathbb{G}_m = R_{F/k}(R_{F_c/F}\mathbb{G}_m) = R_{F/k}(R_{k_c/k}\mathbb{G}_m \times_k F)$, which is a free $\mathbb{Z}$-module of rank rn. We have

$$\widehat{R_{F_c/k}\mathbb{G}_m}\otimes_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}[\mathrm{Gal}(F_c/k)] = \mathbb{Q}[\langle\sigma\rangle\times\langle\tau\rangle] = \mathbb{Q}[\sigma]\otimes_{\mathbb{Q}}\mathbb{Q}[\tau].$$

We choose a character χ_c of $\mathrm{Gal}(F/k)$

$$\chi_c \ : \ \mathrm{Gal}(F/k)\longrightarrow \mathbb{Q}(\zeta_{\ell-1})^\times,\ \chi_c(\sigma)=\zeta_r.$$

For $j=0,1,\dots,r-1$, let

$$e_j^c = \frac{1}{r}\sum_{i=0}^{r-1}\chi_c^j(\sigma^{-i})\sigma^i \in \mathbb{Q}(\zeta_{\ell-1})[\sigma].$$

These e_j's are orthogonal idempotents of $\mathbb{Q}(\zeta_{\ell-1})[\sigma]$. Now, for any positive divisor s of r, we set

$$\varepsilon_s = \sum_{\mathrm{ord}(\zeta_r^j)=s} e_j^c = \frac{1}{r}\sum_{i=0}^{r-1}\mathrm{Tr}_{\mathbb{Q}(\zeta_s)/\mathbb{Q}}\left(\chi_c^{\frac{r}{s}}(\sigma^{-i})\right)\sigma^i,$$

where the sum is taken over the integers j (modulo r) such that the order of ζ_r^j is s, namely over j satisfying $s=r/(r,j)$ and $\mathrm{Tr}_{\mathbb{Q}(\zeta_s)/\mathbb{Q}}$ denotes the trace map. We say that j belongs to s in this situation. Then it is easy to

see that $\varepsilon_s \in \mathbb{Q}[\sigma]$ for all s and they are, indeed, orthogonal idempotents of $\mathbb{Q}[\sigma]$. We have a decomposition of $\widehat{R_{F_c/k}\mathbb{G}_m} \otimes \mathbb{Q}$:

$$\widehat{R_{F_c/k}\mathbb{G}_m} \otimes \mathbb{Q} = \bigoplus_{s|r} (\varepsilon_s \mathbb{Q}[\sigma] \otimes \mathbb{Q}[\tau]) .$$

Let $R(s)$ be an algebraic k-torus whose character module is the $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of $\varepsilon_s\mathbb{Q}[\sigma] \otimes_{\mathbb{Q}} \mathbb{Q}[\tau]$ (cf. the construction of the torus $R(\Phi_d)$ in [15, 5.1]).

In the dual category of k-tori, we have an isogeny.

Proposition 4.1. *There exists an isogeny*

$$\gamma \ : \ \prod_{s|d} R(s) \longrightarrow R_{F/k}(R_{F_c/F}\mathbb{G}_m)$$

defined over F of degree dividing some power of r. In particular, the degree is prime to ℓ.

The assertion on the degree follows by looking at the denominator of the idempotents.

Let $\Lambda \ : \ \mathbb{Z}[\tau] \longrightarrow \mathbb{Z}[\tau]$ be the dual homomorphism of λ. This naturally induces a homomorphism $\Lambda_s = 1 \otimes \Lambda \ : \ \widehat{R(s)} \longrightarrow \widehat{R(s)}$ on the character module of $R(s)$. Therefore we have an induced self-isogeny λ_s of $R(s)$. An easy diagram chase argument shows that there exists an injective homomorphism

$$\begin{aligned} (4.1) \qquad \varphi_s \ : \ R(s)(k)/\lambda_s R(s)(k) &\longrightarrow R_{F_c/k}\mathbb{G}_m(k)/\lambda R_{F_c/k}\mathbb{G}_m(k) \\ &\cong R_{F_c/F}\mathbb{G}_m(F)/\lambda R_{F_c/F}\mathbb{G}_m(F) \\ &= R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F). \end{aligned}$$

Here we use a canonical identification $R_{F_c/F}\mathbb{G}_m(F) = R_{F/k}(R_{F_c/F}\mathbb{G}_m)(k)$.

Now we regard e_j^c as an element of the ℓ-adic group algebra $\mathbb{Z}_\ell[\sigma]$ and reduce modulo ℓ to obtain

$$e_j^c \equiv e_{j'} \pmod{\ell}$$

with some j' belonging to s. We note here that r in the denominator of e_j^c is prime to ℓ. The following proposition is almost obvious from the construction of the k-torus $R(s)$.

Theorem 4.2. *If j belongs to s, then there is j' that also belongs to s such that we have a group isomorphism*

$$e_j \left(R(s)(k)/\lambda_s R(s)(k)\right) \cong e_{j'} \left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right)$$

induced by φ_s in (4.1).

Proof. If j belongs to s, we have $e_j^c \varepsilon_s = e_j^c$. Therefore we have a map from $e_j\,(R(s)(k)/\lambda_s R(s)(k))$ to $e_{j'}\left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right)$. Since $\deg\gamma$ and $\deg\lambda_s$ are coprime, we have the above isomorphism by taking the quotients. □

This theorem means that an inverse image of a k-rational point of a k-torus $R(s)$ essentially generates an $M_\ell(r,s)$-extension. Hence we may consider Theorems 3.1 and 4.2 as a non-abelian Kummer theory. But we should note that, for a general $P \in R(s)(k)$, the extension $F(\lambda^{-1}(P))/k$ is not necessarily a Galois extension. We have to take an e_j-component (see the proof of Theorem 3.1).

Remark 4.3. Let E be an elliptic curve defined over k having a k-rational ℓ-torsion point P. The isogeny $\lambda : E \longrightarrow E' = E/\langle P\rangle$ defined over k induces an injective homomorphism

$$E'(F)/\lambda(E(F)) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k_{\mathrm{sep}}/F), \ker\lambda(k))$$

for any field F containing k. Suppose that F/k is a Galois extension. If we decompose $E'(F)$ by the action of $\mathrm{Gal}(F/k)$, we have a similar construction of metacyclic extensions. If $\mathrm{Aut}(E)$ is compatible with $\mathrm{Gal}(F/k)$, we can also interpret each eigenspace as a twist of E (see [8]). For example, if F/k is a quadratic extension with Galois group $\langle\sigma\rangle$, then the subspace of $E'(F)/\lambda(E(F))$ on which σ acts by -1 is coming from the group of k-rational points on the quadratic twist of E' by F/k.

Although we cannot expect to obtain all such extensions by this single homomorphism, it is shown in [13] and [12] that varying such E's over $\mathbb{Q}$ gives all $D_5 = M_5(2,2)$-extensions over $\mathbb{Q}$.

5. Nakano and Sase's construction

In this section, we compare our result with Nakano and Sase's ([14]). As in the previous sections, let

$$\mathrm{Gal}(F/k) = \langle\sigma\rangle, \quad \mathrm{Gal}(F_c/F) = \langle\tau\rangle$$

and we may regard as

$$\mathrm{Gal}(F_c/k) = \langle\sigma\rangle \times \langle\tau\rangle.$$

Here we impose a condition for the generator τ to satisfy $\zeta_\ell^\tau = \zeta_\ell^{\nu_k(\tau)}$ by the isomorphism (2.5). For a positive integer j prime to s and less than s, let $E(s,j)$ be the fixed subfield of F_c by the subgroup generated by $\tau^{\frac{n}{s}j}\sigma$:

$$E(s,j) = F_c^{\left\langle \tau^{\frac{n}{s}j}\sigma\right\rangle}.$$

We have $[E(s,j):k] = n/s$. Define $\varepsilon = \dfrac{1}{n}\displaystyle\sum_{i=0}^{n-1} \nu_k(\tau^{-i})\tau^i \in \mathbb{F}_\ell[\tau]$. Nakano and Sase prove the following theorem.

Theorem 5.1 (Nakano-Sase [14])**.** *Let L/F be a cyclic extension of degree ℓ. Suppose that L/k is a Galois extension. Take $\alpha \in F_c^\times$ satisfying $L_c = F_c(\sqrt[\ell]{\alpha})$. Then L/k is an $M_\ell(r,s)$-extension if and only if the class of α belongs to $\varepsilon\left(E(s,j)^\times/E(s,j)^{\times\ell}\right)$ for some j prime to s.*

We shall show the following proposition to make clear the relationship to our result.

Proposition 5.2. *If j belongs to s, then there is a surjective homomorphism*

$$e_j\left(R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)\right) \longrightarrow \varepsilon\left(E(s,j')^\times/E(s,j')^{\times\ell}\right)$$

for some j' belonging to s.

Proof. We fix an isomorphism $\phi_k : R_{k_c/k}\mathbb{G}_m \longrightarrow \mathbb{G}_{m,k_c}^n$ defined over k_c. Let $P \in R_{k_c/k}\mathbb{G}_m(F)$ and $\phi_k(P) = (\alpha_1,\dots,\alpha_n)$. Then by [10, Proposition 6.3] we have

$$F_c(\lambda^{-1}(P)) = F_c\left(\sqrt[\ell]{\varepsilon\alpha_1}\right). \tag{5.1}$$

Hence a map sending $\overline{P} \in R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F)$ to $\overline{\alpha_1} \in F_c^\times/F_c^{\times\ell}$ is a well-defined homomorphism. We write α for α_1 for simplicity. If P belongs to the e_j-component, then $P^\sigma \equiv P^{\chi^j(\sigma)} \pmod{\lambda R_{k_c/k}\mathbb{G}_m(F)}$ holds. This yields that $\alpha^\sigma \equiv \alpha^{\chi^j(\sigma)} \pmod{F_c^{\times\ell}}$, because τ and σ commute. Since j belongs to s, the order of $\chi^j(\sigma)$ in $\mathbb{F}_\ell^\times$ is s. Choose j' so that

$$\chi^j(\sigma)\nu_F^{j'}(\tau^{\frac{n}{s}}) \equiv 1 \pmod{\ell}$$

holds. Then it is easy to observe that j' also belongs to s and we have

$$(\varepsilon\alpha)^{\tau^{\frac{n}{s}j'}\sigma} \equiv (\varepsilon\alpha)^{\nu_F^{j'}(\tau^{\frac{n}{s}})\chi^j(\sigma)} \equiv \varepsilon\alpha \pmod{F_c^{\times\ell}}.$$

It follows that the class of $\varepsilon\alpha$ is in $\varepsilon\left(E(s,j')^\times/E(s,j')^{\times\ell}\right)$. Thus we can define a map sending P to the class of $\varepsilon\alpha$. By the construction, this map is a group homomorphism. It remains to show that the map is surjective. Take an element $\alpha \in E(s,j')$ whose class belongs to $\varepsilon\left(E(s,j')^\times/E(s,j')^{\times\ell}\right)$. Let $P = \phi_F^{-1}(\alpha,\alpha^\tau,\dots,\alpha^{\tau^{r-1}})$. Then P maps to the class of $\varepsilon\alpha = \alpha$. This completes the proof of the proposition. □

Since the degree $[F_c:F]$ is prime to ℓ, the expression (5.1) gives a lot of information about the extension $F(\lambda^{-1}(P))/F$. In particular, if F is a number field, then the extension is unramified outside the prime ideals dividing

ℓ and $n\varepsilon\alpha$ (note that n is also prime to ℓ). Furthermore the extension is trivial if and only if $\varepsilon\alpha \in F_c^{\times\ell}$.

Combining with the classical Kummer theory, we obtain the following criterion for isomorphic fields.

Corollary 5.3. *Let P and P' be two points in $R_{k_c/k}\mathbb{G}_m(F)$ and α and α' corresponding elements in $F_c^\times$. Then two fields $F(\lambda^{-1}(P))$ and $F(\lambda^{-1}(P'))$ are isomorphic if and only if $\varepsilon\alpha$ and $\varepsilon\alpha'$ generate the same subgroup in $F_c^\times/F_c^{\times\ell}$.*

6. Examples

In this section, we give explicit examples of Theorems 3.1 and 4.2.

Example 6.1. Let $k = \mathbb{Q}_c^+$ be the maximal real subfield of $\mathbb{Q}_c$. A linear polynomial $\mathscr{P}(t) = \dfrac{\ell+1}{2} + \dfrac{1-\ell}{2}t$ defines an endomorphism of $R_{\mathbb{Q}_c/\mathbb{Q}_c^+}\mathbb{G}_m$ of degree ℓ and we have a Kummer theory $\kappa_{\mathbb{Q}_c^+}$. If F is a quadratic extension of k different from $\mathbb{Q}_c$, then we have

$$\kappa_k \times F \ : \ R_{k_c/k}\mathbb{G}_m(F)/\lambda R_{k_c/k}\mathbb{G}_m(F) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k_s/F), \ker\lambda(k)).$$

Note that if $F = \mathbb{Q}_c$, we have a classical Kummer theory over F instead (see Remark 3.2). The tori in Proposition 4.1 are explicitly given as

$$R(1) = R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \text{ and } R(2) = \ker(N_{F_c/\mathbb{Q}_c} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \to R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m).$$

We have an isogeny

$$\gamma \ : \ R(1) \times R(2) \longrightarrow R_{F_c/\mathbb{Q}}\mathbb{G}_m$$

of degree 2 corresponding to the group algebra decomposition

$$\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] \cong \left(\frac{1-\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] \oplus \left(\frac{1+\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})].$$

Let $P \in R_{F_c/F}\mathbb{G}_m(F)$ and $L_P = F(\lambda^{-1}(P))$. The extension L_P/F is a cyclic extension of degree ℓ. Theorems 3.1 and 4.2 imply that

$$P \in \mathrm{Im}\,\varphi_0 \Longrightarrow L_P/\mathbb{Q}_c^+ \text{ is a } C_{2\ell}\text{-extension};$$
$$P \in \mathrm{Im}\,\varphi_1 \Longrightarrow L_P/\mathbb{Q}_c^+ \text{ is a } D_\ell\text{-extension}.$$

A construction of dihedral extensions over $\mathbb{Q}_c^+$ is also studied in [5]. In their paper, the authors use a clever transformation to obtain a simple family of generic polynomials. Whereas polynomials arising from our construction are less simple, they can be computed systematically and contain more arithmetical information such as irreducibility of them.

For a special case of $\ell = 3$, we have $k = \mathbb{Q}$ and a method to compute an explicit generic polynomial defining D_3-extensions by this Kummer construction is briefly explained in [11].

Example 6.2. Let $\ell = 5$ and $k = \mathbb{Q}$. We take a quartic cyclic extension F over $\mathbb{Q}$ disjoint from $\mathbb{Q}_c$. Then $\mathrm{circ}(1, 1, -1, 0)$ induces a Kummer duality over $\mathbb{Q}$, hence over F. We have

$$R(1) = R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m,$$
$$R(2) = \ker\left(N_{F_c^{\langle\sigma^2\rangle}/\mathbb{Q}_c} : R_{F_c^{\langle\sigma^2\rangle}/\mathbb{Q}}\mathbb{G}_m \to R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m\right),$$

and

$$R(4) = \ker\left(N_{F_c/F_c^{\langle\sigma^2\rangle}} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \to R_{F_c^{\langle\sigma^2\rangle}/\mathbb{Q}}\mathbb{G}_m\right).$$

There is an isogeny

$$\gamma \ : \ R(1) \times R(2) \times R(4) \longrightarrow R_{F_c/\mathbb{Q}}\mathbb{G}_m$$

of degree 4. In this case, the rational points of torus $R(4)$ decomposes to the e_1 and e_3-components if we pass into the quotient by λ. Let $P \in R_{F_c/F}\mathbb{G}_m(F)$ and $L_P = F(\lambda^{-1}(P))$ as in the previous example. Then from our theorems, it follows

$$P \in \mathrm{Im}\,\varphi_1 \Longrightarrow L_P/\mathbb{Q} \text{ is a } C_{20}\text{-extension};$$
$$P \in \mathrm{Im}\,\varphi_2 \Longrightarrow L_P/\mathbb{Q} \text{ is an } M_5(4,2)\text{-extension};$$
$$P \in \mathrm{Im}\,\varphi_4 \Longrightarrow L_{e_iP}/\mathbb{Q} \text{ is an } F_{20}\text{-extension for } i = 1, 3.$$

Note that $M_5(4, 2)$ is *not* a transitive permutation group of degree 5. It is isomorphic to $C_4 \times D_5$ and a polynomial of degree 20 over the base field is required to define it.

Let F' be the unique quadratic intermediate field of F/k. Let k' be an alias for F'. Then we have the following relations between idempotents:

$$e_0(F/k') = e_0(F/\mathbb{Q}) + e_2(F/\mathbb{Q});$$
$$e_1(F/k') = e_1(F/\mathbb{Q}) + e_3(F/\mathbb{Q}).$$

Each idempotent of F/k' corresponds to

$$R(1) = R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \text{ and } R(2) = \ker(N_{F'_c/\mathbb{Q}_c} : R_{F'_c/\mathbb{Q}}\mathbb{G}_m \to R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m),$$

respectively as in Example 6.1. We have C_{10} and D_5-extensions over k' corresponding to each torus. The extension relations in Lemma 3.4 are given by $e_0(F'/\mathbb{Q}) \longrightarrow e_0(F/\mathbb{Q})$ and $e_1(F'/\mathbb{Q}) \longrightarrow e_2(F/\mathbb{Q})$. These relations correspond to the extensions from C_{10} to C_{20} and from D_5 to $M_5(4, 2)$, respectively.

We can compute a cyclic polynomial of L_P/F by the method in [9]. In our case, for a parameter $\phi_F(P) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha_1, \alpha_1^\tau, \alpha_1^{\tau^2}, \alpha_1^{\tau^3})$, it

is given by

$$T^5 + \frac{1}{10}\mathrm{Tr}((\zeta^3+\zeta^2-2)\alpha_1\alpha_3)T^3 + \frac{1}{25}\mathrm{Tr}((\zeta^3-3\zeta^2-2\zeta-1)\alpha_1\alpha_2\alpha_3)T^2$$
$$+ \frac{1}{100}\Big(4\alpha_1\alpha_2\alpha_3\alpha_4 + 4\mathrm{Tr}((\zeta^3+\zeta^2)\alpha_1^2\alpha_2\alpha_3) + 4\mathrm{Tr}((-\zeta^3+\zeta^2+1)\alpha_2^2\alpha_4^2)$$
$$-\mathrm{Tr}((\zeta^3+\zeta^2+1)\alpha_1^2\alpha_3^2 + (-\zeta^3-\zeta^2)\alpha_2^2\alpha_4^2)\Big)T$$
$$+ \frac{1}{625N}\Big(\mathrm{Tr}((-\zeta^3-3\zeta^2-4\zeta-2)\alpha_1^4\alpha_2^2\alpha_3^3) + 5\mathrm{Tr}((2\zeta^2+2\zeta+1)\alpha_1^3\alpha_2^2\alpha_3^3\alpha_4)$$
$$+5\mathrm{Tr}((\zeta^3+\zeta^2+2\zeta+1)\alpha_1^3\alpha_2^2\alpha_3^2\alpha_4^2)\Big) \in F[T],$$

where $\zeta = \zeta_5$ and Tr is the trace map with respect to the group generated by $\tau : \zeta \mapsto \zeta^3$ and N is the norm of α_1. We use a computer algebra system Magma [1] to calculate this polynomial and others in this paper. For any $\alpha = \alpha_1 \in F_c^\times$, a new parameter $e_1\alpha \equiv \alpha^4(\alpha^\sigma)^3(\alpha^{\sigma^2})(\alpha^{\sigma^3})^2 \pmod{F_c^{\times 5}}$ gives an equation over F defining a Frobenius extension over $\mathbb{Q}$, if it is irreducible. To be more explicit, let $F = \mathbb{Q}(a)$ where a is a root of $x^4 - 4x^2 + 2$. The extension $F/\mathbb{Q}$ is a cyclic quartic extension. We take

$$\alpha = (a^3-2a)\zeta + (a^3-3a-1)\zeta^3 + (a^3-3a+1)\zeta^4 + 0\cdot\zeta^2$$

This is a generator of a prime ideal of F_c lying above 43. Then a polynomial for the new parameter $e_1\alpha$ is

$$T^5 + \frac{1}{147008443}(194882430a^2 - 1023328667)T^3$$
$$+ \frac{1}{17094005}(-1849922a^3 + 9747040a)T^2$$
$$+ \frac{1}{108057411566421245}(-238719986420786572a^2 + 935734522878575728)T$$
$$+ \frac{1}{17076753216164011682789400125}(-2154173871765196191502013659 2a^3$$
$$+ 7012758515384142329774543963 2a).$$

This polynomial defines a cyclic quintic extension over F which is an F_{20}-extension over $\mathbb{Q}$. The relative discriminant of the ring of integers of the splitting field has a factorization $\mathfrak{p}_5^8\mathfrak{p}_{43}^4$, where $\mathfrak{p}_p$ is a prime ideal of F lying above p. This is what we can expect from the parameter.

As we noted in Section 2.2, apart from $\ell = 3, 5$, there are Kummer theories for $\ell = 7$ and 11 over $\mathbb{Q}$. These Kummer theories enable us to construct all the metacyclic extensions over $\mathbb{Q}$ for the following groups:

$$C_{14}, D_7, C_{21}, F_{21}, C_{42}, M_7(6,2), M_7(6,3), F_{42}, C_{22}, F_{22},$$
$$C_{55}, C_{110}, M_{11}(10,2), M_{11}(10,5), F_{110}.$$

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. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. **XI**. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[4] M. Hall, Jr., *The theory of groups*. Chelsea Publishing Co., New York, 1976.

[5] K. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*. Number theory and its applications (Kyoto, 1997), Dev. Math., vol. **2**, 165–181. Kluwer Acad. Publ., Dordrecht, 1999.

[6] M. Imaoka and Y. Kishi, *On dihedral extensions and Frobenius extensions*. Galois theory and modular forms, Dev. Math., vol. **11**, 195–220. Kluwer Acad. Publ., Boston, MA, 2004.

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

[8] M. Kida, *Galois descent and twists of an abelian variety*. Acta Arith. **73** (1995), no. 1, 51–57.

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

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

[11] ———, *A Kummer theoretic construction of an S_3-polynomial with given quadratic subfield*. Interdisciplinary Information Sciences **16** (2010), 17–20.

[12] M. Kida, Y. Rikuna, and A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*. Int. J. Number Theory **6** (2010), 691–704.

[13] O. Lecacheux, *Constructions de polynômes génériques à groupe de Galois résoluble*. Acta Arith. **86** (1998), no. 3, 207–216.

[14] S. Nakano and M. Sase, *A note on the construction of metacyclic extensions*. Tokyo J. Math. **25** (2002), no. 1, 197–203.

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

Masanari Kida
University of Electro-Communications
1-5-1 Chofugaoka Chofu
Tokyo 182-8585 Japan
E-mail: kida@sugaku.e-one.uec.ac.jp