ELEMENTARY EXPLICIT SOLUTIONS TO EMBEDDING PROBLEMS WITH CYCLIC KERNEL

NAOYA HASHIMOTO

Abstract. In this paper we consider embedding problems given by central extensions with cyclic kernel. We construct their explicit solutions by using the product of certain 1-cochains, obtained from the vanishing of the obstructions. We also give a simple way to obtain proper solutions from a weak solution and another general field extension.

1. Introduction

Let m be an integer > 1, and let F be a field of characteristic prime to m, containing the group μ_m of m-th roots of unity. Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. Given a central extension

$$1 \longrightarrow \mu_m \xrightarrow{\iota} \tilde{G} \xrightarrow{\pi} G \longrightarrow 1\,, \tag{1.1}$$

we consider a Galois extension E/F with $E \supset K$ and an isomorphism $\varphi\colon \mathrm{Gal}(E/F) \to \tilde{G}$ such that $\pi \circ \varphi = \mathrm{res}_K$, where res_K is the canonical restriction homomorphism from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. We call such an extension E/F a *proper solution*, or simply a *solution* to the *embedding problem* given by K/F and (1.1). We say the embedding problem is *solvable* if it has a solution.

The purpose of this paper is to give an explicit construction of a solution E/F. Several results have been obtained in particular situations: for example, in the case where there is a homomorphism $G \to \mathrm{PSL}(A)$ for a central simple F-algebra A of degree m, Crespo [1] expressed a solution in terms of reduced norms. Swallow [13] and Vela [14] generalized Crespo's results in their own way. There are many results on the case where m is prime and G is an m-group. Especially, in the case $G = (\mathbb{Z}/m\mathbb{Z})^k$, $k \in \mathbb{N}$, Massy [6] and Swallow [12] gave methods to get explicit solutions. Quer [10] generalized some results in [6] to the case where G is an abelian group. Mináč and Swallow [8] also generalized some results in [6], using Galois module structures.

To construct a solution explicitly, we use 1-cochains $(\xi_\sigma)_{\sigma\in G}$ obtained from the vanishing of obstructions to these problems. We consider the product $z \coloneqq \prod_{\sigma\in G} \xi_\sigma$. If m is equal to the order of G (we denote it by n), we easily see that solutions have a form $K(\sqrt[m]{r\eta z^{-1}})/F$ $(r \in F^\times)$, where $\eta \in K^\times$ is an element determined by the extension (1.1). Our goal (Theorem 1) is to show that we can construct solutions in the same way even if $m \neq n$. Note that we only assume $m \mid n$ and $\mu_m \subset F^\times$, in particular we don't require $\mu_n \subset K^\times$. In addition, if m is prime and G is a non-cyclic abelian m-group, we can take 1 as η (Proposition 2).

The organization of this paper is as follows. We show our main result on the construction of *weak solutions* to the embedding problem in Section 2. In Section 3, we give an explicit construction of proper solutions to the problem by using a weak solution and a $\mathbb{Z}/m\mathbb{Z}$ -extension of F (Proposition 1). We illustrate our method with some examples in Section 4.

Convention: For a Galois extension K/F, we denote by ${}^\sigma x$ the action of $\sigma \in \mathrm{Gal}(K/F)$ on $x \in K$.

2020 *Mathematics Subject Classification.* 12F10, 12F12, 12G05.

2. Main results

Let m be an integer > 1, and let F be a field of characteristic prime to m, containing the group μ_m of m-th roots of unity. Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. We consider the embedding problem given by K/F and the central extension

$$1 \longrightarrow \mu_m \xrightarrow{\iota} \tilde{G} \xrightarrow{\pi} G \longrightarrow 1. \tag{2.1}$$

First we recall weak solutions to embedding problems.

Definition 1 ([5, p.34]). A *weak solution* to the embedding problem given by K/F and (2.1) is a Galois extension E/F which contains K/F together with an injective homomorphism $\varphi\colon \mathrm{Gal}(E/F) \hookrightarrow \tilde{G}$ such that $\pi \circ \varphi = \mathrm{res}_K$. Here res_K is the canonical restriction homomorphism from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. If the embedding problem has a weak solution, we say that it is *weakly solvable.*

A proper solution to the embedding problem is also clearly a weak solution.

Let $c \in Z^2(G, \mu_m)$ be a 2-cocycle such that its cohomology class $[c] \in H^2(G, \mu_m)$ corresponds to the extension (2.1). It is well-known that the embedding problem given by K/F and (2.1) is weakly solvable if and only if $\iota([c]) = 1$ holds for the homomorphism $\iota\colon H^2(G, \mu_m) \to H^2(G, K^\times)$ induced by the inclusion $\mu_m \subset K^\times$. Let $\mathrm{Br}(F)$, $\mathrm{Br}(K)$ be the Brauer groups of F, K respectively, and let $\mathrm{Br}(K/F)$ be the kernel of the canonical homomorphism $\mathrm{Br}(F) \to \mathrm{Br}(K)$; $[A] \mapsto [A \otimes_F K]$. We call $\psi(\iota([c])) \in \mathrm{Br}(K/F)$ the *obstruction* to the embedding problem, where ψ is the isomorphism from $H^2(G, K^\times)$ to $\mathrm{Br}(K/F)$. If $K(\sqrt[m]{\omega})/F\,(\omega \in K^\times)$ is a weak solution, we have a family $(\lambda_\sigma)_{\sigma\in G}$ with values in $K^\times$ such that ${}^\sigma\omega = \omega\lambda_\sigma^m$ for all $\sigma \in G$ and that the 2-cocycle $(\sigma, \tau) \mapsto \lambda_\sigma {}^\sigma\lambda_\tau \lambda_{\sigma\tau}^{-1} \in \mu_m$ represents $[c]$. Moreover, all the weak solutions are $K(\sqrt[m]{r\omega})/F$, $r \in F^\times$ (cf. [5, Theorem 2.4.1]).

Let $n = |G|$. In the following, we assume that m divides n.

We define a map χ from G to μ_m by

$$\chi(\sigma) \coloneqq \prod_{\tau\in G} c(\sigma, \tau)\,.$$

Then we have the following lemmas.

Lemma 1. *The map χ only depends on the cohomology class of such a 2-cocycle c.*

Proof. Let $c' \in Z^2(G, \mu_m)$ be a 2-cocycle contained in the cohomology class of c. Then there exists a family $(\theta_\sigma)_{\sigma\in G}$ of elements of μ_m such that $c'(\sigma, \tau) = \theta_\sigma {}^\sigma\theta_\tau \theta_{\sigma\tau}^{-1} \cdot c(\sigma, \tau)$ for all $\sigma, \tau \in G$. Therefore, we have

$$\prod_{\tau\in G} c'(\sigma, \tau) = \prod_{\tau\in G} c(\sigma, \tau) \cdot \prod_{\tau\in G} \theta_\sigma \cdot \frac{\prod_{\tau\in G} \theta_\tau}{\prod_{\tau\in G} \theta_{\sigma\tau}} = \prod_{\tau\in G} c(\sigma, \tau) \cdot 1 \cdot 1 = \prod_{\tau\in G} c(\sigma, \tau).$$

□

Lemma 2. *$\chi\colon G \to \mu_m$ is a group homomorphism and also is a 1-cocycle.*

Proof. Since G operates on μ_m trivially, we only have to check that χ is a homomorphism. Since c is a 2-cocycle of G with values in μ_m, we get

$$\frac{\chi(\sigma\rho)}{\chi(\sigma)\chi(\rho)} = \frac{\prod_\tau c(\sigma\rho, \tau)}{\prod_\tau c(\sigma, \tau) \prod_\tau c(\rho, \tau)} = \frac{\prod_\tau c(\sigma, \rho\tau)}{\prod_\tau c(\sigma, \tau) \prod_\tau c(\sigma, \rho)} = 1$$

by a simple calculation. □

By Hilbert Satz 90, there exists an element η of $K^\times$ such that

$$\chi(\sigma) = \prod_{\tau \in G} c(\sigma, \tau) = \frac{{}^\sigma\eta}{\eta}$$

for arbitrary $\sigma \in G$. Using η, we can describe a solution to the embedding problem explicitly:

Theorem 1. *Let $c \in Z^2(G, \mu_m)$ be a 2-cocycle whose class $[c] \in H^2(G, \mu_m)$ corresponds to the extension (2.1). Assume the embedding problem given by K/F and (2.1) is weakly solvable. By this assumption, we set a family (ξ_σ) of elements of $K^\times$ with $\xi_\sigma {}^\sigma\xi_\tau \xi_{\sigma\tau}^{-1} = c(\sigma, \tau)$ for all $\sigma, \tau \in G$. Suppose η is an element of $K^\times$ with ${}^\sigma\eta/\eta = \prod_{\tau\in G} c(\sigma,\tau)$ for all $\sigma \in G$, and put $\alpha = \left(\prod_{\sigma\in G} \xi_\sigma\right)^{-1} \eta$. Then there exists an element $r \in F^\times$ such that $K(\sqrt[n]{r\alpha})/F$ is a weak solution to this embedding problem.*

Proof. Let σ be an arbitrary element of G. By a simple calculation, we get

$$\frac{{}^\sigma\eta}{\eta} = \prod_{\tau\in G} c(\sigma,\tau) = \prod_{\tau\in G} \frac{\xi_\sigma {}^\sigma\xi_\tau}{\xi_{\sigma\tau}} = \frac{\left(\prod_{\tau\in G}\xi_\sigma\right) {}^\sigma\!\left(\prod_{\tau\in G}\xi_\tau\right)}{\prod_{\tau\in G}\xi_{\sigma\tau}} = \frac{\xi_\sigma^n {}^\sigma\!\left(\prod_{\tau\in G}\xi_\tau\right)}{\prod_{\tau\in G}\xi_{\sigma\tau}}.$$

Hence we have ${}^\sigma\alpha/\alpha = \xi_\sigma^n$.

Let $\overline{K}$ be a separable closure of K and let $\overline{G} = \mathrm{Gal}(\overline{K}/F)$, $N = \mathrm{Gal}(\overline{K}/K)$. We have $\inf([c]) = 1$, where $\inf\colon H^2(G,\mu_m) \to H^2(\overline{G},\mu_m)$ is the inflation map. As a part of the 5-term exact sequences,

$$F^\times/F^{\times m} \longrightarrow (K^\times/K^{\times m})^G \xrightarrow{\delta_m} H^2(G,\mu_m) \xrightarrow{\inf} H^2(\overline{G},\mu_m)$$

and

$$F^\times/F^{\times n} \longrightarrow (K^\times/K^{\times n})^G \xrightarrow{\delta_n} H^2(G,\mu_n^N) \xrightarrow{\inf} H^2(\overline{G},\mu_n)$$

are exact. Here δ_m is a map which sends the class of $x \in K^\times$ to the class of 2-cocycle $c'(\sigma,\tau) = \lambda_\sigma {}^\sigma\lambda_\tau \lambda_{\sigma\tau}^{-1}$, where λ_σ are elements of $K^\times$ with ${}^\sigma x = x\lambda_\sigma^m$ for each $\sigma \in G$. We define δ_n similarly, and μ_n^N denotes the subgroup of μ_n which is stable under the operation of N.

Let $\varphi\colon H^2(G,\mu_m) \to H^2(G,\mu_n^N)$ be a map induced by the inclusion $\mu_m \subset \mu_n^N$. Then we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
F^\times/F^{\times m} & \longrightarrow & (K^\times/K^{\times m})^G & \xrightarrow{\delta_m} & H^2(G,\mu_m) & \xrightarrow{\inf} & H^2(\overline{G},\mu_m) \\
\downarrow{\scriptstyle n/m} & & \downarrow{\scriptstyle n/m} & & \downarrow{\scriptstyle \varphi} & & \downarrow \\
F^\times/F^{\times n} & \longrightarrow & (K^\times/K^{\times n})^G & \xrightarrow{\delta_n} & H^2(G,\mu_n^N) & \xrightarrow{\inf} & H^2(\overline{G},\mu_n).
\end{array}$$

Here the symbol n/m denotes the map induced by $x \mapsto x^{n/m}$. Then we see $\inf(\varphi([c])) = 1$ and $\delta_n([\alpha]_n) = \varphi([c])$, where $[\alpha]_n$ is the class of α in $(K^\times/K^{\times n})^G$.

By the assumption, there exists an element $\beta \in K^\times$ such that $K(\sqrt[m]{\beta})/F$ is a weak solution. Then $\delta_m([\beta]_m) = [c]$ holds, where $[\beta]_m$ is the class of β in $(K^\times/K^{\times m})^G$. Now the commutativity of the diagram shows $\delta_n([\beta^{n/m}]_n) = \varphi(\delta_m([\beta]_m)) = \varphi([c]) = \delta_n([\alpha]_n)$, which implies $[\beta^{n/m}]_n = [r\alpha]_n$ for some $r \in F^\times$. Therefore $\beta^{n/m}x_0^n = r\alpha$ for some $x_0 \in K^\times$. Clearly $\sqrt[m]{\beta}x_0$ is one of the n-th roots of $r\alpha$, and the theorem holds since $K(\sqrt[m]{\beta}x_0) = K(\sqrt[m]{\beta})$. $\square$

Remark 1. Let $x' \in H^1(N,\mu_m)$ correspond to $[x]_m$ by the isomorphism $H^1(N,\mu_m) \simeq K^\times/K^{\times m}$. We have $\delta_m([x]_m) = (tg(x'))^{-1}$, where tg is the *transgression* map in [9, Proposition 1.6.6]. We also have $\delta_n([x]_n) = (tg(x''))^{-1}$, where $x'' \in H^1(N,\mu_n)$ corresponds to $[x]_n$ by the isomorphism $H^1(N,\mu_n) \simeq K^\times/K^{\times n}$.

Remark 2. It is also known that one of the weak solutions is given by $y = \sum_\sigma \xi_\sigma^{-m} \cdot \sigma(x)$ for some $x \in K^\times$ (for example, see Quer [10, p.187] and Vela [14, proof of Proposition 8.2(b)]). Our solution is related to Crespo's results [1], rather than this one.

See Section 4 for details to determine η and r.

3. From weak solutions to proper solutions

We keep the notation of the previous section.

For a weak solution $K(\sqrt[m]{\beta})/F$ to be a *proper* solution to the embedding problem given by K/F and (2.1), it is necessary and sufficient that the class $[\beta]$ of β in $K^\times/K^{\times m}$ is of order m. Therefore, if there is an element r of $F^\times$ such that $[K(\sqrt[m]{r\beta})\colon K]=m$, then the problem has a proper solution. The existence of such an r follows from the existence of $g\in F^\times$ in the following proposition:

Proposition 1. *Let g be an element of $F^\times$ whose class $[g]$ in $F^\times/F^\times\cap K^{\times m}$ is of order m, and let β be an element of $K^\times$ whose class $[\beta]$ in $K^\times/K^{\times m}$ is of order ℓ. If g and β satisfy the equalities*

$$[\beta]^{\mathbb{Z}}\cap[g]^{\mathbb{Z}}=[\beta^{\ell/h}]^{\mathbb{Z}}=[g^{m/h}]^{\mathbb{Z}},\qquad [\beta^{\ell/h}]=[g^{m/h}]$$

for some divisor h of ℓ, then the class $[\beta g^{1-m/\ell}]$ in $K^\times/K^{\times m}$ is of order m.

Proof. We just apply the following lemma to the case where $M=K^\times/K^{\times m}$, $\omega=\beta$, $\theta=g$, $u=h$, $w=m$ and $v=\ell$:

Lemma 3. *Let M be an abelian group (written additively), and let $\theta,\omega\in M$ be of order w and v, respectively. If v is a divisor of w and equalities*

$$\mathbb{Z}\theta\cap\mathbb{Z}\omega=\mathbb{Z}\frac{w}{u}\theta=\mathbb{Z}\frac{v}{u}\omega,\qquad \frac{w}{u}\theta=\frac{v}{u}\omega$$

hold for some divisor u of v, then the map

$$\psi\colon\mathbb{Z}/w\mathbb{Z}\times\mathbb{Z}/\left(\frac{v}{u}\right)\mathbb{Z}\longrightarrow\mathbb{Z}\theta+\mathbb{Z}\omega\subset M,\qquad (x,y)\longmapsto x\theta+y\left(-\frac{w}{v}\theta+\omega\right)$$

is a group isomorphism. In particular, the order of $\left(1-\frac{w}{v}\right)\theta+\omega\in M$ is equal to w.

Proof. It is easy to verify that ψ is well-defined and is a group homomorphism. ψ is surjective because θ and ω are images of $(1,0)$ and $(w/v,1)$, respectively.

We show that ψ is injective. Let A,B be integers such that $A\theta+B\left(-(w/v)\theta+\omega\right)=0$ holds. Since $\left(A-B(w/v)\right)\theta=-B\omega$ and $\mathbb{Z}\theta\cap\mathbb{Z}\omega=\mathbb{Z}(v/u)\omega$ we have $B\in(v/u)\mathbb{Z}$. This implies $A\theta=0$, and then $A\in w\mathbb{Z}$. Hence ψ is injective. □

4. Application to some examples

In this section, we illustrate our method with some central extensions, which are, cyclic groups of square order (see 4.1), the group $D_4\curlywedge\mathbb{Z}/4\mathbb{Z}$ (see 4.2) and the modular group M_{16} (see 4.3).

Before applying our methods to each example, we summarize how to construct weak solutions, and show useful results in particular situations.

Suppose m is an integer >1, F is a field of characteristic prime to m containing the group μ_m of m-th roots of unity, and K/F is a finite Galois extension with Galois group $G=\mathrm{Gal}(K/F)$ such that $n:=|G|$ is a multiple of m. We consider the embedding problem given by K/F and the central extension

$$1\longrightarrow\mu_m\xrightarrow{\iota}\tilde{G}\xrightarrow{\pi}G\longrightarrow 1,\qquad (2.1)$$

and suppose that the problem is weakly solvable. To apply Theorem 1 for construction of weak solutions, we need the following three steps:

(1) Find a 2-cocycle $c \in Z^2(G, \mu_m)$ whose cohomology class corresponds to the extension (2.1), and find a family $(\xi_\sigma)_{\sigma \in G}$ of elements of $K^\times$ with $\xi_x {}^x\xi_y \xi_{xy}^{-1} = c(x,y)$ for all x, y in G.

(2) Calculate $\chi(\sigma) = \prod_{\tau \in G} c(\sigma,\tau)$ for each $\sigma \in G$, and find $\eta \in K^\times$ such that ${}^\sigma\eta/\eta = \chi(\sigma)$ ($\forall \sigma \in G$). Then calculate $\alpha = \left(\prod_{\sigma \in G} \xi_\sigma\right)^{-1} \eta$.

(3) Find $r \in F^\times$ such that $K(\sqrt[n]{r\alpha})/F$ is a weak solution to the embedding problem.

In (1), we can use a section $f\colon G \to \tilde{G}$ of (2.1) and the 2-cocycle $c \in Z^2(G, \mu_m)$ defined by $\iota(c(\sigma,\tau)) = f(\sigma)f(\tau)f(\sigma\tau)^{-1}$ ($\sigma, \tau \in G$), which we call *the associated 2-cocycle with* f. Finding a family (ξ_σ) is the most difficult step. For the argument of finding (ξ_σ) using norm properties when m is prime and G is abelian, see Quer [10].

For (2), we note that $\chi(\sigma)$ does not depend on the choice of f by Lemma 1. The following proposition is useful to find η in some cases:

Proposition 2. *Let $M = \langle\sigma_1\rangle \times \cdots \times \langle\sigma_k\rangle$ be an abelian group, where $\sigma_i \in M$ and $m \mid \mathrm{ord}(\sigma_i)$ $(1 \le i \le k)$. Regarding μ_m as an M-module by the trivial action, let $c \in Z^2(M, \mu_m)$ be a 2-cocycle whose cohomology class corresponds to a central extension*

$$1 \longrightarrow \mu_m \overset{\iota}{\longrightarrow} \tilde{M} \overset{\pi}{\longrightarrow} M \longrightarrow 1.$$

We define the map χ from M to μ_m by $\chi(\sigma) = \prod_{\tau \in M} c(\sigma,\tau)$. Then we have the following:

(1) If $k \ge 2$, we have $\chi(\sigma) = 1$ for all $\sigma \in M$.

(2) If $k = 1$, we have $\chi(\sigma_1^i) = \zeta^i$ $(0 \le i \le |M|-1)$ for some $\zeta \in \mu_m$.

Proof. Put $\mathrm{ord}(\sigma_i) = m\ell_i$ ($\ell_i \in \mathbb{Z}$, $1 \le i \le k$). Let s_i ($1 \le i \le k$) be an element of $\tilde{M}$ such that $\pi(s_i) = \sigma_i$. We define the section $f\colon M \to \tilde{M}$ by $\sigma_1^{h_1} \cdots \sigma_k^{h_k} \longmapsto s_1^{h_1} \cdots s_k^{h_k}$ $(0 \le h_i \le m\ell_i - 1)$. Let $c \in Z^2(M, \mu_m)$ be the associated 2-cocycle with f.

We define $\zeta_i \in \mu_m$ $(1 \le i \le k)$ by $s^{m\ell_i} = \iota(\zeta_i)$, and if $k \ge 2$ we define $\zeta_{u,v} \in \mu_m$ $(1 \le u < v \le k)$ by $s_v s_u = \iota(\zeta_{u,v}) s_u s_v$. By these definitions we have

$$c(\sigma_i, \sigma_1^{h_1} \cdots \sigma_k^{h_k}) = \zeta_i^{X_i} \zeta_{1,i}^{h_1} \zeta_{2,i}^{h_2} \cdots \zeta_{i-1,i}^{h_{i-1}}, \qquad X_i = \begin{cases} 0 & (h_i \ne m\ell_i - 1) \\ 1 & (h_i = m\ell_i - 1) \end{cases}$$

for $0 \le h_j \le m\ell_j - 1$, $1 \le j \le k$. Therefore, we have

$$\chi(\sigma_i) = \prod_{j=1}^{k} \prod_{h_j=0}^{m\ell_j - 1} \left(\zeta_i^{X_i} \zeta_{1,i}^{h_1} \zeta_{2,i}^{h_2} \cdots \zeta_{i-1,i}^{h_{i-1}} \right) = \zeta_i^{Y_i} \prod_{u=1}^{i-1} \zeta_{u,i}^{Z_{u,i}},$$

where

$$Y_i = \prod_{j \ne i} m\ell_j, \qquad Z_{u,i} = \{0 + 1 + \cdots + (m\ell_u - 1)\} \cdot \prod_{j \ne u} m\ell_j = \frac{1}{2} m\ell_u (m\ell_u - 1) \prod_{j \ne u} m\ell_j.$$

If $k \ge 2$, $Y_i, Z_{u,i}$ are multiples of m, and we have $\chi(\sigma_i) = 1$ for $1 \le i \le k$. Since χ is a homomorphism (Lemma 2), the assertion (1) holds.

If $k = 1$, we have $M = \langle\sigma_1\rangle$ and $\chi(\sigma_1) = \zeta_1$. Then the assertion (2) follows from Lemma 2. □

By Proposition 2, we can take $\eta = 1$ if $G \simeq G_1 \times \cdots \times G_k$ $(k \ge 2)$, where G_i $(1 \le i \le k)$ are cyclic and $|G_i|$ are multiples of m. If G is cyclic, we can take $\eta = \sqrt[m]{x}$ for some $x \in F^\times$.

In (3), we first search for $r' \in F^\times$ and $\gamma \in K^\times$ with $\gamma^{n/m} = r'\alpha$. We see that $\eta_\sigma := {}^\sigma\gamma\gamma^{-1}\xi_\sigma^{-m}$ is an element of $K^\times$ and also is an n/m-th root of unity. If $\eta_\sigma = 1$ ($\forall \sigma \in G$), clearly $K(\sqrt[m]{\gamma})/F$ itself is a weak solution to the embedding problem. Otherwise, $K(\sqrt[m]{\gamma})/F$ may not be a weak solution. We have the following criterion:

Lemma 4. *Let γ be an element of $K^\times$ with ${}^\sigma\gamma/\gamma = \xi_\sigma^m \eta_\sigma$, $\eta_\sigma \in \mu_{n/m} \cap K^\times$ for all $\sigma \in G$. Then $K(\sqrt[m]{\gamma})/F$ is a weak solution to the embedding problem if and only if $\eta_\sigma \in K^{\times m}$ for all $\sigma \in G$.*

Proof. *"if"* -part: There exists a family $(x_\sigma)_{\sigma\in G}$ with $x_\sigma \in K^\times$ and $x_\sigma^m = \eta_\sigma$ for all $\sigma \in G$. Then we have $x_\sigma {}^\sigma x_\tau x_{\sigma\tau}^{-1} \in \mu_m$ for all $\sigma, \tau \in G$. The 2-cocycle $c' \in Z^2(G, \mu_m)$ given by $c'(\sigma,\tau) = (\xi_\sigma x_\sigma)\,{}^\sigma(\xi_\tau x_\tau)(\xi_{\sigma\tau}x_{\sigma\tau})^{-1}$ is contained in the cohomology class of c. Hence we see that $K(\sqrt[m]{\gamma})/F$ is a weak solution to the embedding problem.

"only if" -part: For an element $a \in K^\times$ with ${}^\sigma a/a = \eta_\sigma^{-1}\,(\forall\sigma \in G)$, $K(\sqrt[m]{\gamma a})/F$ is a weak solution to the embedding problem. If $K(\sqrt[m]{\gamma})/F$ is also a weak solution, $a = r\gamma^{k-1}y^m$ holds for some $r \in F^\times$, $y \in K^\times$ and some integer k prime to m. We have

$$\eta_\sigma^{-1} = \frac{{}^\sigma a}{a} = \left(\frac{{}^\sigma y}{y}\right)^m \left(\frac{{}^\sigma\gamma}{\gamma}\right)^{k-1} = \left(\frac{{}^\sigma y}{y}\right)^m \left(\xi_\sigma^{k-1}\right)^m \eta_\sigma^{k-1}.$$

If we denote $z_\sigma = ({}^\sigma y y^{-1}\xi_\sigma^{k-1})^{-1}$ and take $u, v \in \mathbb{Z}$ such that $ku + mv = 1$, we obtain $\eta_\sigma = (z_\sigma^u \eta_\sigma^v)^m$ since $\eta_\alpha^{ku} = z_\sigma^{mu}$. This proves the assertion. □

If F is a field of characteristic $\neq 2$, we will denote by $(a,b) \in \mathrm{Br}(F)$ the class of the quaternion algebra generated over F by two elements i, j with

$$i^2 = a, \quad j^2 = b, \quad ji = -ij$$

for elements $a, b \in F^\times$. It is well-known that $(a,b) = 1$ holds if and only if b is in the image of the norm of $F(\sqrt{a})/F$.

4.1. Cyclic group of order m^2: Extension $1 \longrightarrow \mu_m \longrightarrow \mathbb{Z}/m^2\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 1$.

Let F be a field with characteristic prime to m, containing the group μ_m of m-th roots of unity. Let $K = F(\sqrt[m]{a})$, where a is an element of $F^\times$ whose class of a in $F^\times/F^{\times m}$ is of order m. Then $G := \mathrm{Gal}(K/F) \simeq \mathbb{Z}/m\mathbb{Z}$. Let σ be a generator of G, and we define $\zeta \in \mu_m$ by ${}^\sigma(\sqrt[m]{a}) = \zeta\sqrt[m]{a}$. We consider the embedding problem given by K/F and the extension

$$1 \longrightarrow \mu_m \xrightarrow{\zeta\mapsto s^m} \mathbb{Z}/m^2\mathbb{Z} \xrightarrow{s\mapsto\sigma} G \longrightarrow 1, \tag{4.1}$$

where s is a generator of $\mathbb{Z}/m^2\mathbb{Z}$. We remark that every weak solution to this embedding problem is a proper solution, since we easily see that no proper subgroup of $\mathbb{Z}/m^2\mathbb{Z}$ can be the Galois group of a weak solution.

If we take the section $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m^2\mathbb{Z}$ of (4.1) defined by $f(\sigma^i) = s^i$ $(0 \le i \le m-1)$, the 2-cocycle $c \in Z^2(G, \mu_m)$ associated with f is given by

$$c(\sigma^i, \sigma^j) = \begin{cases} 1 & (i+j < m) \\ \zeta & (i+j \ge m) \end{cases}$$

for $0 \le i, j \le m-1$.

It is known that this embedding problem has a solution if and only if there exists an element ρ of $K^\times$ with $\rho\,{}^\sigma\rho \cdots {}^{\sigma^{m-1}}\rho = \zeta$ (for example, see Vela [14, Theorem 7.1]). We suppose that this problem is solvable, and take an element $\rho \in K^\times$ such that $\rho\,{}^\sigma\rho \cdots {}^{\sigma^{m-1}}\rho = \zeta$. If we put

$$\xi_{\sigma^i} = \rho\,{}^\sigma\rho \cdots {}^{\sigma^{i-1}}\rho \qquad (0 \le i \le m-1),$$

we get $\xi_x {}^x\xi_y \xi_{xy}^{-1} = c(x,y)$ for all $x, y \in G$.

On the other hand, we have $\chi(\sigma^i) = \prod_{j=0}^{m-1} c(\sigma^i, \sigma^j) = \zeta^i$ for $0 \le i, j \le m-1$, and we can take $\eta = \sqrt[m]{a}$ as an element with ${}^{\sigma^i}\eta/\eta = \zeta^i$ for all $0 \le i \le m-1$. Therefore,

$$\alpha = \sqrt[m]{a} \cdot \left(\prod_{i=0}^{m-1} (\rho \, {}^{\sigma}\rho \cdots {}^{\sigma^{i-1}}\rho) \right)^{-1} = \sqrt[m]{a} \cdot \left(\rho^{m-1} \, {}^{\sigma}\rho^{m-2} \cdots {}^{\sigma^{m-2}}\rho \right)^{-1},$$

and we see that one of the solutions is $K(\sqrt[m]{\alpha})/F$. An equivalent expression is

$$K\left(\sqrt[m]{\sqrt[m]{a} \cdot \rho \, {}^{\sigma}\rho^2 \cdots {}^{\sigma^{m-2}}\rho^{m-1}} \right) \Big/ F.$$

Remark. This solution is known, and also stated heuristically by Massy ([6, Théorème 3] and [7, Théorème 1]) in the case where m is prime. In our viewpoint, the solution is a consequence of Theorem 1.

4.2. An extension of D_4: $1 \longrightarrow \mu_2 \longrightarrow D_4 \curlywedge \mathbb{Z}/4\mathbb{Z} \longrightarrow D_4 \longrightarrow 1$.

Let F be a field with characteristic $\neq 2$, and let K/F be a Galois extension with $G := \mathrm{Gal}(K/F) \simeq D_4$, where $D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$ is the dihedral group. Then we have $K = F(\sqrt{r(A + B\sqrt{a})}, \sqrt{b})$, where $a, b \in F^\times$ are quadratically independent, $A^2 - aB^2 = ab$, $r, B \in F^\times$ and $A \in F$. Let $\sigma, \tau \in G$ be given by

$$\sigma\colon \sqrt{r(A + B\sqrt{a})} \longmapsto \frac{\sqrt{a}\sqrt{b}}{A + B\sqrt{a}} \sqrt{r(A + B\sqrt{a})} = \sqrt{r(A - B\sqrt{a})}, \quad \sqrt{b} \longmapsto \sqrt{b},$$

$$\tau\colon \sqrt{r(A + B\sqrt{a})} \longmapsto \sqrt{r(A + B\sqrt{a})}, \qquad \sqrt{b} \longmapsto -\sqrt{b},$$

whence $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$.

Let $D_4 \curlywedge \mathbb{Z}/4\mathbb{Z}$ be the pull-back

$$D_4 \curlywedge \mathbb{Z}/4\mathbb{Z} = D_4 \times_{(g,h)} \mathbb{Z}/4\mathbb{Z} = \{(x, y) \in D_4 \times \mathbb{Z}/4\mathbb{Z} \mid g(x) = h(y)\},$$

where $g\colon D_4 \to \mathbb{Z}/2\mathbb{Z}$ and $h\colon \mathbb{Z}/4\mathbb{Z} = \langle z \rangle \to \mathbb{Z}/2\mathbb{Z}$ are epimorphisms with kernel $\langle \sigma^2, \tau \rangle$ and $\langle z^2 \rangle$, respectively. It has a presentation

$$D_4 \curlywedge \mathbb{Z}/4\mathbb{Z} = \langle u, v, w \mid u^4 = v^2 = w^2 = 1,\ vu = u^3vw,\ w \text{ is central} \rangle.$$

We consider the embedding problem given by K/F and

$$1 \longrightarrow \mu_2 \xrightarrow{-1 \mapsto w} D_4 \curlywedge \mathbb{Z}/4\mathbb{Z} \xrightarrow[\pi]{u \mapsto \sigma,\ v \mapsto \tau} D_4 \longrightarrow 1\,. \tag{4.2}$$

It is known that the obstruction to this embedding problem is $(a, -1) \in \mathrm{Br}(F)$ ([3, Example 4.6]).

We remark that every weak solution to this embedding problem is proper. Indeed, we can easily verify that the exact sequence (4.2) does not split (i.e., there exists no homomorphism $f'\colon D_4 \to D_4 \curlywedge \mathbb{Z}/4\mathbb{Z}$ with $\pi \circ f' = \mathrm{id}$), which implies that D_4 cannot be the Galois group of a weak solution. It is obvious that the other proper subgroups of $D_4 \curlywedge \mathbb{Z}/4\mathbb{Z}$ are not Galois groups of weak solutions.

We take the section $f\colon D_4 \to D_4 \curlywedge \mathbb{Z}/4\mathbb{Z}$ of (4.2) defined by $\sigma^i\tau^j \mapsto u^iv^j$ ($0 \le i \le 3$, $0 \le j \le 1$). Then we have

$$f(\sigma^i\tau^j)f(\sigma^k\tau^l) = u^iv^ju^kv^l = u^iu^{3jk}v^jv^lw^{jk} = u^{[i+3jk]_4}v^{[j+l]_2}w^{[jk]_2}$$

$$f(\sigma^i\tau^j\sigma^k\tau^l) = f(\sigma^{[i+3jk]_4}\tau^{[j+l]_2}) = u^{[i+3jk]_4}v^{[j+l]_2}$$

for $0 \le i, k \le 3$, $0 \le j, l \le 1$. Here $[x]_y$ denotes the remainder of an integer $x \ge 0$ divided by an integer $y \ge 1$. Hence we see that the associated 2-cocycle is given by

$$c(\sigma^i\tau^j, \sigma^k\tau^l) = \begin{cases} -1 & (j, k) = (1, 1), (1, 3) \\ 1 & \text{otherwise} \end{cases}.$$

We also see $\chi(x) = 1$ for all $x \in G$ and therefore we can take $\eta = 1$.

Suppose this embedding problem is solvable. Let ρ be an element of $F(\sqrt{a})$ with $\rho\, {}^{\sigma}\rho = -1$. Then we have $\xi_x {}^x\xi_y \xi_{xy}^{-1} = c(x,y)$ for all $x, y \in G$ if we put

$$\xi_{\sigma^i\tau^j} = \rho\, {}^{\sigma}\rho \cdots {}^{\sigma^{i-1}}\rho \quad (0 \le i \le 3, 0 \le j \le 1)\,.$$

Now we have $\alpha = 1 \cdot \left(\prod_{\sigma \in D_4} \xi_\sigma\right)^{-1} = \rho^{-4}$. Then $\sqrt[8]{\alpha} = \sqrt{\rho^{-1}}$, and we see

$$\frac{{}^{\sigma}(\rho^{-1})}{\rho^{-1}} = \frac{\rho}{{}^{\sigma}\rho} = -\rho^2 = -\xi_\sigma^2, \qquad \frac{{}^{\tau}(\rho^{-1})}{\rho^{-1}} = 1 = \xi_\tau^2\,.$$

From these calculations we obtain ${}^x(\rho^{-1}\sqrt{a}) = \rho^{-1}\sqrt{a} \cdot \xi_x^2$ for all $x \in G$, and we conclude that $K(\sqrt{\rho\sqrt{a}})/F$ is a solution to this problem.

Remark 1. $K(\sqrt{\rho})/F$ is also a solution to this problem if and only if $K^\times$ contains μ_4 (Lemma 4).

Remark 2. Grundman, Smith and Swallow [2, Section 4.4] also explain constructions of $D_4 \curlywedge \mathbb{Z}/4\mathbb{Z}$-extensions, by considering the extension $1 \to \mu_m \to D_4 \curlywedge \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 1$.

4.3. Extension of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: $1 \longrightarrow \mu_2 \longrightarrow M_{16} \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$.

Let F be a field with characteristic $\neq 2$, and let K/F be a Galois extension with $G := \mathrm{Gal}(K/F) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then we have $K = F(\sqrt{u(v + w\sqrt{a})}, \sqrt{b})$, where $a, b \in F^\times$ are quadratically independent, $v^2 - aw^2 = a$, $u, w \in F^\times$ and $v \in F$. Let $\sigma, \tau \in G$ be given by

$${}^{\sigma}\left(\sqrt{u(v + w\sqrt{a})}\right) = \sqrt{u(v - w\sqrt{a})}, \qquad {}^{\tau}(\sqrt{b}) = -\sqrt{b}, \qquad \frac{{}^{\sigma}(\sqrt{b})}{\sqrt{b}} = \frac{{}^{\tau}(\sqrt{u(v + w\sqrt{a})})}{\sqrt{u(v + w\sqrt{a})}} = 1\,.$$

The center of $M_{16} := \langle s, t \mid s^8 = t^2 = 1, ts = s^5 t\rangle$ is $\{1, s^2, s^4, s^6\}$. We consider the embedding problem given by K/F and the extension

$$1 \longrightarrow \mu_2 \xrightarrow{-1 \mapsto s^4} M_{16} \xrightarrow[t \mapsto \tau]{s \mapsto \sigma} G \longrightarrow 1\,. \tag{4.3}$$

As in the previous examples, every weak solution to this embedding problem is also a proper solution.

We take the section $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to M_{16}$ of (4.3) defined by $\sigma^i\tau^j \mapsto s^i t^j$ $(i = 0, 1, 2, 3,\ j = 0, 1)$. Then the associated 2-cocycle $c \in Z^2(G, \mu_2)$ is

$$c(\sigma^i\tau^j, \sigma^k\tau^l) = \begin{cases} (-1)^{jk+1} & (i + k \ge 4) \\ (-1)^{jk} & (i + k < 4) \end{cases} \tag{4.4}$$

for $0 \le i, k \le 3$ and $0 \le j, l \le 1$.

The obstruction to this embedding problem is $(a, 2b)(-1, uv)$, and it is known that $(a, 2b)(-1, uv) = 1$ if and only if $-b^2$ is a norm of the extension L/F, where $L = K(\sqrt{u(v + w\sqrt{a})})$ (cf. Ledet [3, p.1263, Remark]). We suppose that this problem is solvable.

Let $\rho \in L$ be an element with $\prod_{i=0}^{3} {}^{\sigma^i}\rho = -b^2$. Then we have $\xi_x {}^x\xi_y \xi_{xy}^{-1} = c(x, y)$ $(\forall x, y \in G)$ if we put

$$\xi_{\sigma^i\tau^j} = \frac{\rho\, {}^{\sigma}\rho \cdots {}^{\sigma^{i-1}}\rho}{\sqrt{b}^i} \qquad (i = 0, 1, 2, 3,\ j = 0, 1)\,.$$

By Proposition 2 we have $\eta = 1$, and we get

$$\alpha = \frac{b^6}{\rho^6 ({}^{\sigma}\rho)^4 ({}^{\sigma^2}\rho)^2}\,.$$

Therefore, there exists an element r of $F^\times$ such that $\sqrt[4]{r\alpha} \in K$ and $K(\sqrt[8]{r\alpha})/F$ is a solution to this problem.

We consider the condition on r. In the following, we assume $v \neq 0$ (for the case $v = 0$, see Remark 3). Since $b^2 r\rho^2({}^{\sigma^2}\rho)^2 \in K^4$, the form of r is one of the followings:

$$r = C^2, \quad C^2 a, \quad C^2 b, \quad C^2 ab \qquad (C \in F^\times).$$

Let $z \in K$ be a square root of r. Then a solution is $K\left(\sqrt{\dfrac{b}{\rho^\sigma\rho\sqrt{z\rho\,{}^{\sigma^2}\rho}}}\right)\Big/F$, and $\sqrt{z\rho\,{}^{\sigma^2}\rho} \in K$ holds.

Let $\delta := \dfrac{b}{\rho^\sigma\rho\sqrt{z\rho\,{}^{\sigma^2}\rho}}$, and suppose $K(\sqrt{\delta})/F$ is a solution to this embedding problem. We may assume ${}^x\delta/\delta = \xi_x^2$ for arbitrary $x \in G$. Since ${}^\sigma(\delta^2)/\delta^2 = \xi_\sigma^4$ and ${}^\tau(\delta^2)/\delta^2 = 1$, we have $z = C\sqrt{a}$ for some $C \in F^\times$.

It remains to determine C. Let $\gamma := \sqrt{C\sqrt{a}\rho\,{}^{\sigma^2}\rho}$. We may assume $\gamma\,{}^\sigma\gamma = bC\sqrt{a}$. Also, since $\gamma^2 \in F(\sqrt{a})$, $\gamma \in K$ has degree 2 over $F(\sqrt{a})$, and we have ${}^\tau\gamma = \pm\gamma$, and ${}^{\sigma^2}\gamma = \pm\gamma$. Here, clearly we need ${}^\tau\gamma = \gamma$ for ${}^\tau\delta/\delta = 1 = \xi_\tau^2$. If we assume ${}^{\sigma^2}\gamma = \gamma$, then we have $\gamma \in F(\sqrt{a}, \sqrt{b})$, which contradicts $\gamma\,{}^\sigma\gamma = bC\sqrt{a}$. Hence we see ${}^{\sigma^2}\gamma = -\gamma$.

Therefore $\gamma \in F(\sqrt{u(v + w\sqrt{a})})$, and we can put $\gamma = A\sqrt{u(v + w\sqrt{a})} + B\sqrt{u(v - w\sqrt{a})}$, where A, B are elements of F. Putting $\rho\,{}^{\sigma^2}\rho = X + Y\sqrt{a}\,(X, Y \in F)$, we have

$$\gamma^2 = C\sqrt{a}(X + Y\sqrt{a}), \qquad \gamma\,{}^\sigma\gamma = bC\sqrt{a}.$$

Comparing coefficients, we see that the equalities

$$\begin{aligned} YaC &= uv(A^2 + B^2)\,, \\ XC &= u\{w(A^2 - B^2) + 2AB\}\,, \\ bC &= u\{(A^2 - B^2) - 2wAB\} \end{aligned}$$

hold.

Now the problem comes down to solving these equations. Then we obtain $\sqrt{C\sqrt{a}\rho\,{}^{\sigma^2}\rho} = A\sqrt{u(v + w\sqrt{a})} + B\sqrt{u(v - w\sqrt{a})} \in K$ and get a solution to this embedding problem.

Special case of 4.3. As a special case, we also assume $uv = a$ and $b = w$. In this case, we have $\rho\,{}^\sigma\rho\,{}^{\sigma^2}\rho\,{}^{\sigma^3}\rho = -b^2$ for

$$\rho = 1 + \frac{1}{u}\sqrt{u(v + w\sqrt{a})}\,.$$

Then $X = 1 - v/u$, $Y = -w/u$ and the preceding equalities are

$$\begin{aligned} -waC &= u^2 v(A^2 + B^2)\,, \\ (u - v)C &= u^2\{w(A^2 - B^2) + 2AB\}\,, \\ wC &= u\{(A^2 - B^2) - 2wAB\}\,. \end{aligned}$$

Since $w \neq 0$, the solution of this equation is $A = wB$, $C = -(u/w)(w^2 + 1)B^2$. Thus we have

$$\begin{aligned} \delta &= \frac{b}{\rho^\sigma\rho(w\sqrt{u(v + w\sqrt{a})} + \sqrt{u(v - w\sqrt{a})})} \\ &= \frac{bu}{(u + \sqrt{a} + \sqrt{u(v + w\sqrt{a})} + \sqrt{u(v - w\sqrt{a})})(w\sqrt{u(v + w\sqrt{a})} + \sqrt{u(v - w\sqrt{a})})} \end{aligned}$$

and $K(\sqrt{\delta})/F$ is a solution to this embedding problem. Also, $K(\sqrt{bu\delta^{-1}})/F$ is a solution and

$$bu\delta^{-1} = \left(u + \sqrt{a} + \sqrt{u(v + w\sqrt{a})} + \sqrt{u(v - w\sqrt{a})}\right)\left(w\sqrt{u(v + w\sqrt{a})} + \sqrt{u(v - w\sqrt{a})}\right).$$

Remark 1. Ledet [4] also constructs a solution in a different way, using the equivalence of quadratic forms. Based on results for $\mathbb{Z}/8\mathbb{Z}$-extension in Schneps [11], Grundman, Smith and Swallow [2] also gave another construction of M_{16}-extension in the case $(a, 2b) = (-1, uv) = 1$.

Remark 2. If $\mu_4 \subset F^\times$, the extension $K\left(\sqrt[4]{\dfrac{\sqrt{a}b^3}{\rho^3({}^\sigma\rho)^2({}^{\sigma^2}\rho)}}\right)\Big/F$ is a weak solution to the embedding problem given by K/F and the extension

$$1 \longrightarrow \mu_4 \xrightarrow{\zeta_4 \mapsto \overline{(1,g)}} \widetilde{G}' \xrightarrow[\overline{(t,1)} \mapsto \tau]{\overline{(s,1)} \mapsto \sigma} G \longrightarrow 1,$$

where $\widetilde{G}'$ is the central product of M_{16} and $\mathbb{Z}/4\mathbb{Z} = \langle g \rangle$ over subgroups $\{1, s^4\}$ and $\{1, g^2\}$, i.e.

$$\widetilde{G}' = M_{16} \times \mathbb{Z}/4\mathbb{Z} \Big/ \{(1,1), (s^4, g^2)\}.$$

Indeed, if we define the section $f\colon G \to \widetilde{G}'$ by $\sigma^i\tau^j \mapsto (s^it^j, 1)$, the associated 2-cocycle $c \in Z^2(G, \mu_4)$ is clearly given by (4.4).

Moreover, if $\mu_8 \subset F^\times$, the extension $K(\sqrt[8]{\alpha})/F$ itself is a weak solution to the embedding problem given by K/F and the extension

$$1 \longrightarrow \mu_8 \xrightarrow{\zeta_8 \mapsto \overline{(1,h)}} \widetilde{G}'' \xrightarrow[\overline{(t,1)} \mapsto \tau]{\overline{(s,1)} \mapsto \sigma} G \longrightarrow 1,$$

where $\widetilde{G}''$ is the central product of M_{16} and $\mathbb{Z}/8\mathbb{Z} = \langle h \rangle$ over subgroups $\{1, s^4\}$ and $\{1, h^4\}$, i.e.

$$\widetilde{G}'' = M_{16} \times \mathbb{Z}/8\mathbb{Z} \Big/ \{(1,1), (s^4, h^4)\}.$$

Remark 3. If $v = 0$, solutions to this problem can be obtained explicitly. Without loss of generality, we can assume $\mu_4 \subset F^\times$ and $K = F(\sqrt[4]{a}, \sqrt{b})$, and let $\sigma, \tau \in G$ be given by

$${}^\sigma(\sqrt[4]{a}) = \zeta\sqrt[4]{a}, \quad {}^\tau(\sqrt{b}) = -\sqrt{b}, \quad \frac{{}^\sigma(\sqrt{b})}{\sqrt{b}} = \frac{{}^\tau(\sqrt[4]{a})}{\sqrt[4]{a}} = 1,$$

where ζ is a primitive 4th root of unity. The obstruction is $(a, 2b)$, and we can take $p, q \in F$ which satisfies $(p + q\sqrt{a})(p - q\sqrt{a}) = 2b$. Then $\rho\,{}^\sigma\rho\,{}^{\sigma^2}\rho\,{}^{\sigma^3}\rho = -b^2$ holds for

$$\rho = \frac{(1+\zeta)(p - q\sqrt{a})}{2} = \frac{(1+\zeta)b}{p + q\sqrt{a}},$$

and $\xi_x {}^x\xi_y \xi_{xy}^{-1} = c(x, y)$ holds for arbitrary $x, y \in G$ if we take

$$\xi_{\tau^j} = 1, \qquad \xi_{\sigma\tau^j} = \frac{(1+\zeta)\sqrt{b}}{p + q\sqrt{a}}, \qquad \xi_{\sigma^2\tau^j} = \zeta, \qquad \xi_{\sigma^3\tau^j} = \frac{(\zeta - 1)\sqrt{b}}{p + q\sqrt{a}} \qquad (j = 0, 1).$$

Now we get

$$\alpha \coloneqq \left(\prod_{x \in G} \xi_x\right)^{-1} = \frac{(p + q\sqrt{a})^4}{-4b^2}$$

and we have $\sqrt[8]{r\alpha} = \sqrt{(p + q\sqrt{a})\sqrt[4]{a}}$ for $r = -4ab^2$. We see that $K(\sqrt{(p + q\sqrt{a})\sqrt[4]{a}})/F$ is a solution. This solution agrees with the one shown in [5, (7.3.6)].

Acknowledgments

The author would like to thank Professor Takeshi Kajiwara for valuable discussions and his constant support. The author would also like to thank the referees of this paper for their valuable suggestions and comments, which have greatly contributed to the improvement of this paper.

References

[1] T. Crespo: *Embedding Galois problems and reduced norms*, Proc. AMS **112** (1991), 637-639.
[2] H. G. Grundman, T. L. Smith, J. R. Swallow: *Groups of order* 16 *as Galois groups*, Expo. Math. **13** (1995), 289-319.
[3] A. Ledet: *On* 2*-groups as Galois groups*, Canad. J. Math. **47** (1995), 1253-1273.
[4] A. Ledet: *Embedding problems and equivalence of quadratic forms,* Math. Scand. **88** (2001), 279-302.
[5] A. Ledet: Brauer type embedding problems, Fields Institute Monographs, vol. 21, American Mathematical Society, Providence, 2005.
[6] R. Massy: *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), 508-535.
[7] R. Massy: *Solutions explicites de problèmes de plongement*, J. of number theory **20** (1985), 299-314.
[8] J. Mináč, J. Swallow: *Galois embedding problems with cyclic quotient of order p*, Isr. J. Math. **145** (2005), 93-112.
[9] J. Neukirch, A. Schmidt, K. Wingberg: Cohomology of number fields, 2nd edition, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2008.
[10] J. Quer: *Embedding problems over abelian groups and an application to elliptic curves*, J. Algebra **237** (2001), 186-202.
[11] L. Schneps: *On cyclic field extensions of degree* 8, Math. Scand. **71** (1992), 24-30.
[12] J. R. Swallow: *Central p-extensions of $(p, p, \ldots, p)$-type Galois Groups*, J. Algebra **186** (1996), 277-298.
[13] J. R. Swallow: *Solutions to central embedding problems are constructible*, J. Algebra **184** (1996), 1041-1051.
[14] M. Vela: *Explicit solutions of Galois embedding problems by means of generalized Clifford algebras*, J. Symb. Comput. **30** (2000), 811-842.

Graduate School of Engineering Science, Yokohama National University, 79-5 Tokiwadai, Hodogaya-ku, Yokohama city, Japan

Email address: hashimoto-naoya-wd@ynu.jp