Canad. Math. Bull. Vol. **66** (2), 2023, pp. 380–394
http://dx.doi.org/10.4153/S0008439522000388

Arithmetically equivalent fields in a Galois extension with Frobenius Galois group of 2-power degree

Masanari Kida

Abstract. Let F_{2^n} be the Frobenius group of degree 2^n and of order $2^n(2^n-1)$ with $n \geq 4$. We show that if $K/\mathbb{Q}$ is a Galois extension whose Galois group is isomorphic to F_{2^n}, then there are $\dfrac{2^{n-1}+(-1)^n}{3}$ intermediate fields of $K/\mathbb{Q}$ of degree $4(2^n-1)$ such that they are not conjugate over $\mathbb{Q}$ but arithmetically equivalent over $\mathbb{Q}$. We also give an explicit method to construct these arithmetically equivalent fields.

1 Introduction

The following theorem concerning coincidence of Hecke L-functions is proved in [6].

Theorem 1.1 *Let p be a prime number. If $K/\mathbb{Q}$ is a Galois extension whose Galois group G is isoclinic to the Heisenberg group of order p^3, then there are $p+1$ abelian normal subgroups H_i $(i=1,\dots,p+1)$ of index p in G and characters χ_i of H_i such that $p+1$ Hecke L-functions $L(\chi_i, s)$ coincide up to a finite number of Euler factors.*

A natural question arises from this theorem.

Question *Are there arbitrarily large number of number fields whose Dedekind zeta functions coincide?*

Two number fields K and K' are called *arithmetically equivalent* (over $\mathbb{Q}$) if the Dedekind zeta functions of K and K' coincide. Conjugate number fields obviously have the same Dedekind zeta functions; thus, we are interested in nonconjugate arithmetically equivalent fields. Many examples of such fields are known until now (see [8, Examples in III.1.b]), but examples of three or more arithmetically equivalent fields seem not to be known. The aim of this paper is to give such examples systematically.

Received by the editors February 27, 2022; revised May 11, 2022, accepted June 7, 2022.
Published online on Cambridge Core June 13, 2022.
This work was supported by JSPS KAKENHI Grant Number 20K03521.
AMS subject classification: **11R42**, 12F12.
Keywords: Dedekind zeta function, arithmetically equivalent fields, Frobenius group, inverse Galois problem.

To state our result more precisely, we introduce some notation. Let $\mathbb{F}_{2^n}$ be a finite field of 2^n elements. We consider the Frobenius group F_{2^n} defined by

$$F_{2^n} = \mathbb{F}_{2^n}^{\times} \ltimes \mathbb{F}_{2^n},$$

where $\mathbb{F}_{2^n}^{\times}$ acts faithfully on $\mathbb{F}_{2^n}$. The group F_{2^n} can be described also as an affine linear group over $\mathbb{F}_{2^n}$:

$$F_{2^n} \cong \mathrm{AGL}_1(\mathbb{F}_{2^n}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{2^n}) \;\middle|\; a \in \mathbb{F}_{2^n}^{\times},\ b \in \mathbb{F}_{2^n} \right\}. \tag{1.1}$$

The Frobenius kernel N is isomorphic to

$$\left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in \mathrm{AGL}_1(\mathbb{F}_{2^n}) \;\middle|\; b \in \mathbb{F}_{2^n} \right\} \cong \mathbb{F}_2^n,$$

and a Frobenius complement H is isomorphic to

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{AGL}_1(\mathbb{F}_{2^n}) \;\middle|\; a \in \mathbb{F}_{2^n}^{\times} \right\} \cong \mathbb{F}_{2^n}^{\times}.$$

Let $K/\mathbb{Q}$ be a Galois extension with Galois group isomorphic to the Frobenius group F_{2^n}. Such an extension $K/\mathbb{Q}$ is called an F_{2^n}-extension. The fixed field L of K by the Frobenius kernel N is a cyclic extension of degree $2^n - 1$ over $\mathbb{Q}$ and $\mathrm{Gal}(K/L)$ is isomorphic to an elementary abelian 2-group of rank n.

Our main theorem is the following.

Theorem 1.2 *Let n be an integer greater than 3. Among intermediate fields M of an F_{2^n}-extension $K/\mathbb{Q}$ with $[M : L] = 4$, there are $\dfrac{2^{n-1} + (-1)^n}{3}$ fields which are not conjugate but arithmetically equivalent.*

As a matter of fact, there are several nonconjugate arithmetically equivalent fields of degree $2^s (s = 2, \ldots, n-2)$ over L inside K. We concentrate the smallest degree fields for simplicity both in the proof and in the construction. Our proof and construction are explicit and specific throughout, and this enables us to find families of a large number of nonconjugate arithmetically equivalent fields explicitly.

The outline of the paper is as follows. In the next section, we prove Theorem 1.2 in a refined form (Theorem 2.4) by using mainly the representation theory of finite groups. In Section 3, we discuss how to construct F_{2^n}-extensions. We show that if a cyclic extension L is constructed, then we can construct infinitely many F_{2^n}-extensions containing L by using Kummer theory (Theorem 3.3). Our discussion here is explicit and constructive for the argument in the following section. In Section 4, we explain how to find nonconjugate arithmetically equivalent fields in an F_{2^n}-extension and give an explicit description of these fields (Proposition 4.1).

Throughout this paper, we use the following notation. We fix an integer n greater than 3. The Frobenius group of degree 2^n and of order $2^n(2^n - 1)$ is denoted by $F_{2^n} = H \ltimes N$ with H and N defined in the above.

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

2 The proof of the main theorem

In this section, we shall prove Theorem 1.2. Let $K/\mathbb{Q}$ be an F_{2^n}-extension. We fix an isomorphism between $\mathrm{Gal}(K/\mathbb{Q})$ and $F_{2^n} = H \ltimes N$ and identify them by the isomorphism. Let L be the fixed field K^N. The extension $L/\mathbb{Q}$ is a cyclic extension of degree $2^n - 1$. The Galois group of K/L is isomorphic to an elementary abelian 2-group N of rank n, since the additive group of the field $\mathbb{F}_{2^n}$ is isomorphic to $\mathbb{F}_2^n$.

In this section, we use the following notation from the representation theory of finite groups. For a finite group G, we denote by $\mathrm{Irr}(G)$ the set of the irreducible character of G and by 1_G the principal character of G. For a character ψ of a subgroup E of G, we denote the induced character from ψ to G by ψ^G and for a character χ of G, the restriction of χ to E by χ_E.

We begin by showing that all intermediate fields M of $K/\mathbb{Q}$ with $[M : L] = 4$ are arithmetically equivalent. By [8, Theorem III.1.3], it suffices to show the following proposition.

Proposition 2.1 *Let n be an integer greater than 3. Let $G = F_{2^n} = H \ltimes N$. If E is a subgroup of N of order 2^{n-2}, then the induced character 1_E^G is independent of the choice of E and hence the characters 1_E^G are equal for all E.*

Note that the group E in Proposition 2.1 is core-free, that is, $\mathrm{Core}_G(E) = \bigcap_{g\in G}(gEg^{-1}) = 1$, and thus the character 1_E^G is a faithful permutation character. This also implies that the Galois closure of K^E coincides with K.

To prove the proposition, we use the following fact on the representation of Frobenius groups, which is a special case of [4, Satz V.16.13].

Lemma 2.2 *The irreducible characters of $F_{2^n} = H \ltimes N$ consist of linear characters μ_i $(i \in \{0, \dots, 2^n - 2\})$ which are extensions of $\eta_i \in \mathrm{Irr}(H)$ with $\ker \mu_i \supset N$ and a character ψ of degree $2^n - 1$ induced from a nontrivial character φ of N such that $\psi_N = \sum_{h\in H} \varphi^h$.*

Proof of Proposition 2.1 We compute the inner product of 1_E^G and $\chi \in \mathrm{Irr}(G)$ by Frobenius reciprocity:

$$(1_E^G, \chi)_G = (1_E, \chi_E)_E = \frac{1}{|E|} \sum_{x\in E} \chi(x^{-1}).$$

Let μ_i and ψ be the characters as in Lemma 2.2. Since $E \subset N$, we have

$$(1_E^G, \mu_i)_G = \frac{2^{n-2}}{|E|} = 1.$$

If $\chi = \psi$, then we can write $\psi = \varphi^G$ with $\varphi(\neq 1_N) \in \mathrm{Irr}(N)$. It is clear that $\psi(1) = [G : N] = 2^n - 1$. For a nontrivial element $x \in E \subset N$, we have

$$\psi(x) = \sum_{h\in H} \varphi(hxh^{-1}) = \sum_{g\in N-\{1\}} \varphi(g) = -1.$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

Here, the second equality holds since the action of H on N is transitive and faithful, and therefore the set $\{hxh^{-1} \mid h \in H\}$ coincides with $N - \{1\}$. Moreover, the third equality follows from the fact that φ is nontrivial. We conclude

$$\begin{aligned}(1_E^G, \psi)_G &= \frac{1}{2^{n-2}} \left(\psi(1) + \sum_{x(\neq 1) \in E} \psi(x) \right) \\ &= \frac{1}{2^{n-2}} (2^n - 1 + (-1)(2^{n-2} - 1)) = 3.\end{aligned}$$

Consequently, we obtain the decomposition of 1_E^G:

$$1_E^G = 3\psi + \sum_{i=0}^{2^n-2} \mu_i,$$

which is independent of the choice of E. This completes the proof of Proposition 2.1. ∎

We have an immediate corollary by [8, Theorem III.1.3].

Corollary 2.3 *All quartic extensions over L contained in K are arithmetically equivalent.*

We now enumerate such quartic fields up to conjugacy. We shall prove a more precise version of Theorem 1.2.

Theorem 2.4 *For each quadratic extension F over L in K, there are $2^{n-1} - 1$ quartic extensions M over L with $F \subset M \subset K$.*

(i) *If n is odd, then they are divided into $\frac{2^{n-1}-1}{3}$ conjugacy classes over $\mathbb{Q}$ containing three fields in each class. By choosing one field from each conjugacy class, $\frac{2^{n-1}-1}{3}$ fields are nonconjugate and arithmetically equivalent.*

(ii) *If n is even, then they are divided into $\frac{2^{n-1}-2}{3}$ conjugacy classes over $\mathbb{Q}$ containing three fields in each class, and the other conjugacy class consists of the remaining one field. By choosing one field from each conjugacy class, $\frac{2^{n-1}+1}{3}$ fields are nonconjugate and arithmetically equivalent.*

We have already showed their arithmetic equivalence in Corollary 2.3. By Galois theory, we only have to prove the following group-theoretic version of Theorem 2.4.

Theorem 2.5 *Let $\mathscr{E}$ be the set of the subgroups of order 2^{n-2} of N. The group G acts on $\mathscr{E}$ through $\mathbb{F}_{2^n}^\times$. Let D be a subgroup of N of order 2^{n-1}. We have $|\mathscr{E} \cap D| = 2^{n-1} - 1$ with obvious abuse of notation.*

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

(i) *If n is odd, then the set $\mathscr{E}$ is divided into $\dfrac{2^{n-1}-1}{3}$ conjugacy classes under G and the classes C satisfy $|C \cap D| = 3$.*

(ii) *If n is even, then the set $\mathscr{E}$ is divided into $\dfrac{2^{n-1}+1}{3}$ conjugacy classes under G, the $\dfrac{2^{n-1}-2}{3}$ conjugacy classes C satisfy $|C \cap D| = 3$, and the rest of the classes C' satisfies $|C' \cap D| = 1$.*

Proof It is well known that the number of t-dimensional subspaces in an s-dimensional vector space over $\mathbb{F}_2$ is given by the q-binomial coefficient with $q = 2$, which we denote by

$$\begin{bmatrix} s \\ t \end{bmatrix} = \frac{(2^s-1)(2^{s-1}-1)\cdots(2^{s-t+1}-1)}{(2^t-1)(2^{t-1}-1)\cdots(2-1)}.$$

Using this formula, we can compute

$$|\mathscr{E}| = \begin{bmatrix} n \\ n-2 \end{bmatrix} = \begin{bmatrix} n \\ 2 \end{bmatrix} = \frac{1}{3}(2^n-1)(2^{n-1}-1)$$

and

$$|\mathscr{E} \cap D| = \begin{bmatrix} n-1 \\ n-2 \end{bmatrix} = \begin{bmatrix} n-1 \\ 1 \end{bmatrix} = 2^{n-1}-1.$$

Now, we identify N with the additive group of $\mathbb{F}_{2^n}$. If g is a generator of $\mathbb{F}_{2^n}^{\times}$ and $E \in \mathscr{E}$, then we can write $E = \{0, g^{i_1}, \dots, g^{i_{2^{n-2}-1}}\}$ with $\{i_1, \dots, i_{2^{n-2}-1}\} \subset \{1, 2, \dots, 2^n-1\}$. For notational convenience, we write it as $E = (i_1, \dots, i_{2^{n-2}-1})$. If we represent $\tau \in G$ by a product $g^\ell v$ ($g^\ell \in H, v \in N$), then it is easy to see that the conjugate E^τ is given by $E^\tau = E^{g^\ell} = (i_1+\ell, \dots, i_{2^{n-2}-1}+\ell)$. We compute the normalizer $N_G(E)$. We have $\tau = g^\ell v \in N_G(E)$ if and only if there exists a permutation $\gamma \in S_{2^{n-2}-1}$ such that

$$i_j + \ell \equiv i_{\gamma(j)} \pmod{2^n-1} \quad (j = 1, \dots, 2^{n-2}-1).$$

Summing up both the sides for j, we obtain

$$(i_1 + \cdots + i_{2^{n-2}-1}) + (2^{n-2}-1)\ell \equiv (i_1 + \cdots + i_{2^{n-2}-1}) \pmod{2^n-1},$$

and this yields $(2^{n-2}-1)\ell \equiv 0 (\text{mod } 2^n-1)$. In this connection, we see

$$\gcd(2^{n-2}-1, 2^n-1) = \gcd(2^n-1, 3) = \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 3, & \text{if } n \text{ is even}. \end{cases}$$

Therefore, if n is odd, then we conclude that $\ell = 0$ and $N_G(E) = N$. Hence, the orbit length of every $E \in \mathscr{E}$ is 2^n-1, and the set $\mathscr{E}$ is divided into $\frac{1}{3}(2^{n-1}-1)$ conjugacy classes.

If n is even, then we obtain $\ell = 0$ or $\dfrac{2^n-1}{3}$. In the latter case, the element g^ℓ in $N_G(E)$ is of order 3. Accordingly, the orbit length of E is either 2^n-1 or $\dfrac{2^n-1}{3}$. Let u

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

(resp. v) be the number of orbits of length $2^n - 1$ $\left(\text{resp. } \frac{2^n - 1}{3}\right)$. It obviously yields

$$u(2^n - 1) + v\frac{2^n - 1}{3} = |\mathscr{E}|. \tag{2.1}$$

We compute the total number of orbits $u + v$ by using the lemma of Burnside–Frobenius [1, Lemma 6.2]. For $x \in G$, if we define

$$\mathrm{Fix}(x) = \{E \in \mathscr{E} \mid E^x = E\},$$

then we have

$$u + v = \frac{1}{|G|} \sum_{x \in G} |\mathrm{Fix}(x)|.$$

As is seen in the above, we have $\mathrm{Fix}(g^i v) = \mathrm{Fix}(g^i)$ if we write $x = g^i v$ with $v \in N$. Moreover, if the order of g^i is neither 1 nor 3, then $\mathrm{Fix}(x) = \varnothing$. Obviously, if the order of g^i is equal to 1, then we have $i = 0$ and $\mathrm{Fix}(1) = \mathscr{E}$.

We now suppose that the order of g^i is 3, and thus $i = (2^n - 1)/3$. Since the minimal polynomial of g^i over $\mathbb{F}_2$ is $X^2 + X + 1$ of degree 2, the irreducible $\langle g^i \rangle$-module B is of dimension 2 over $\mathbb{F}_2$. It is easy to see that B is of the form $\{0, g^t, g^{t+i}, g^{t+2i}\}$ with some $0 \le t \le 2^n - 1$. Since one of $t, t + i, t + 2i$ modulo $2^n - 1$ lies in the first one-third interval, we may assume that $0 \le t < (2^n - 1)/3$. Hence, there are $\frac{2^n - 1}{3}$ distinct irreducible $\langle g^i \rangle$-modules inside N. To compute $|\mathrm{Fix}(g^i)|$, we have to enumerate $(n - 2)$-dimensional $\langle g^i \rangle$- modules inside N, but instead we only have to enumerate the complementary two-dimensional modules by Maschke's theorem [5, Theorem 1.9]. Therefore, we conclude $|\mathrm{Fix}(g^i)| = \frac{2^n - 1}{3}$.

Therefore, it follows that

$$u + v = \frac{2^n}{2^n(2^n - 1)} \sum_{i=0}^{2^n - 2} |\mathrm{Fix}(g^i)| = \frac{1}{2^n - 1}\left(|\mathscr{E}| + 2 \times \frac{2^n - 1}{3}\right) = \frac{2^{n-1} + 1}{3}. \tag{2.2}$$

Solving equations (2.1) and (2.2), we obtain

$$u = \frac{2}{3}(2^{n-2} - 1) \text{ and } v = 1.$$

We conclude that there are $\frac{2}{3}(2^{n-2} - 1)$ conjugacy classes of length $2^n - 1$ and one conjugacy class of length $\frac{2^n - 1}{3}$.

Let $\mathscr{O}$ be an orbit in $\mathscr{E}$. Since G acts on the set of D's transitively by Singer's theorem [3, Theorem 11.3.1], the number $|\mathscr{O} \cap D|$ is independent of the choice of D.

We first consider the case where n is odd. Let $\mathscr{O}_i$ $(i = 1, \ldots, (2^{n-1} - 1)/3)$ be the conjugacy classes. Since

$$\sum_{i=1}^{(2^{n-1}-1)/3} |\mathscr{O}_i \cap D| = |\mathscr{E} \cap D| \tag{2.3}$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

holds, it follows

$$\frac{1}{3}(2^{n-1}-1)|\mathscr{O}_i \cap D| = 2^{n-1}-1.$$

Hence, we conclude that $|\mathscr{O}_i \cap D| = 3$, namely each D contains three conjugate fields.

Next, we consider the case where n is even. Let $\mathscr{O}_i$ $(i = 1,\dots,2(2^{n-2}-1)/3)$ be the conjugacy classes of length 2^n-1, and let $\mathscr{P}$ be the conjugacy class of length $(2^n-1)/3$. If $E \in \mathscr{P}$, then it is invariant by an element of order 3 in $\mathbb{F}_{2^n}^{\times}$. Therefore, such E is contained in three different D's. Since there are 2^n-1 nonconjugate D's, we conclude that $|\mathscr{P} \cap D| = 1$. This also yields an equation like (2.3):

$$\sum_{i=1}^{2(2^{n-2}-1)/3} |\mathscr{O}_i \cap D| = |\mathscr{E} \cap D| - 1.$$

From this, it follows $|\mathscr{O}_i \cap D| = 3$ for all i.

This completes the proof of Theorem 2.5, and thus Theorems 1.2 and 2.4 follow. ■

Remark 2.6 Theorem 1.2 holds even if the base field is not $\mathbb{Q}$. However, in that case, we cannot define the arithmetic equivalence by the coincidence of the Dedekind zeta functions. See [8, Theorem III.1.3].

3 Construction of F_{2^n}-extensions

In this section, we construct F_{2^n}-extensions for every n. The method is an extension of those used in [7, 9], where only metacyclic extensions are constructed.

The method fully works for a general base field k whose characteristic is not 2. Thus, we assume that $G = \mathrm{Gal}(K/k) = F_{2^n} = H \ltimes N$ and $L = K^N$, and that a cyclic extension L/k has been constructed.

In the case $k = \mathbb{Q}$, if we take a prime number ℓ satisfying $\ell \equiv 1 (\mathrm{mod}\ 2^n - 1)$, there is a unique cyclic field L of degree 2^n-1 inside the ℓth cyclotomic field. Furthermore, there exist infinitely many such prime numbers ℓ for each n by Dirichlet's theorem on arithmetic progression.

Let us return to the general case. We now have to construct an elementary abelian 2-extension of degree 2^n over L which is an F_{2^n}-extension over k. We fix a generator g of $\mathbb{F}_{2^n}^{\times}$ and consider the $\mathbb{F}_{2^n}$-valued characters

$$\chi_i : C_{2^n-1} \longrightarrow \mathbb{F}_{2^n}^{\times} \text{ such that } \chi_i(\sigma) = g^i \text{ for } i = 0,\dots,2^n-2.$$

Here, we consider the cyclic group C_{2^n-1} as a Galois group of L/k, and σ is a fixed generator of C_{2^n-1}. In this situation, it is necessary to distinguish $\mathrm{Gal}(L/k)$ and $\mathbb{F}_{2^n}^{\times}$. We define

$$e_i = \sum_{j=0}^{2^n-2} \chi_i(\sigma^{-j})\sigma^j \in \mathbb{F}_{2^n}[C_{2^n-1}].$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

They are the primitive orthogonal idempotents, and we have a direct sum decomposition of the group ring

$$\mathbb{F}_{2^n}[C_{2^n-1}] = \bigoplus_{i=0}^{2^n-2} e_i \mathbb{F}_{2^n}[C_{2^n-1}]$$

into one-dimensional irreducible modules by Maschke's theorem.

We now further define

$$\varepsilon_i = \mathrm{Tr}_{\mathbb{F}_2(\chi_i)/\mathbb{F}_2}(e_i) \in \mathbb{F}_2[C_{2^n-1}], \tag{3.1}$$

where $\mathbb{F}_2(\chi_i)$ is the field generated by the character values of χ_i. There are as many different ε_i as the Galois conjugacy class of the characters $\{\chi_i\}$ (see [5, Lemma 9.17]), and they are nonzero by [5, Corollary 9.22]. If we factor the polynomial $X^{2^n-1} - 1 = \prod_t \phi_t(X)$ into irreducibles in the polynomial ring $\mathbb{F}_2[X]$, then we have a direct sum decomposition over $\mathbb{F}_2$:

$$\mathbb{F}_2[C_{2^n-1}] = \mathbb{F}_2[\sigma] \cong \mathbb{F}_2[X]/(X^{2^n-1} - 1) \cong \bigoplus_t \mathbb{F}_2[X]/(\phi_t(X)).$$

If we choose the index t so that ϕ_t is a minimal polynomial of $\chi_t(\sigma)$, then

$$\varepsilon_i \mathbb{F}_2[\sigma] \cong \bigoplus_{j=0}^{[\mathbb{F}_2(\chi_i):\mathbb{F}_2]-1} \mathbb{F}_{2^n}[X]/(X - \chi_{2^j i}(\sigma)) = \mathbb{F}_2[X]/(\phi_i(X)). \tag{3.2}$$

Hence, we obtain

$$\mathbb{F}_2[C_{2^n-1}] = \bigoplus_t \varepsilon_t \mathbb{F}_2[C_{2^n-1}].$$

Lemma 3.1 *Let the notation be as above. If* $(i, 2^n - 1) = 1$, *then the module* $V_i = \varepsilon_i \mathbb{F}_2[C_{2^n-1}]$ *is an irreducible* $\mathbb{F}_2[C_{2^n-1}]$*-module of dimension* n *over* $\mathbb{F}_2$.

Proof If we assume that $(i, 2^n - 1) = 1$, then the order of χ_i is exactly $2^n - 1$ and the value of χ_i is not contained in any proper subfields of $\mathbb{F}_{2^n}$. Thus, we observe that $\varepsilon_i \mathbb{F}_2[C_{2^n-1}]$ is an n-dimensional subspace over $\mathbb{F}_2$.

Since ε_i's are orthogonal idempotents, V_i is apparently an $\mathbb{F}_2[C_{2^n-1}]$-module.

To show its irreducibility, suppose to the contrary that V_i is not irreducible. There is a proper submodule W of V_i. Since V_i splits over $\mathbb{F}_{2^n}$, the module W also splits over $\mathbb{F}_{2^n}$. Therefore, the character of W is a proper subsum of ε_i. However, such a subsum does not have its values in $\mathbb{F}_2$; therefore, W cannot be defined over $\mathbb{F}_2$. This is a contradiction. ■

It is readily seen that there are $\varphi(2^n - 1)/n$ ε_i's with $(i, 2^n - 1) = 1$, where φ is the Euler's totient function.

Lemma 3.2 *Let the notation be as in Lemma 3.1. If* $(i, 2^n - 1) = 1$, *we have*

$$C_{2^n-1} \ltimes V_i \cong F_{2^n}$$

as abstract groups.

Proof By (1.1), it suffices to show that $C_{2^n-1} \ltimes V_i$ is isomorphic to $\mathrm{AGL}_1(\mathbb{F}_{2^n})$.

By the isomorphism (3.2), we identify V_i with $\mathbb{F}_2[X]/(\phi_i(X))$, where $\phi_i(X)$ is the minimal polynomial of $g^i = \chi_i(\sigma)$ and hence is of degree n. We define a map κ from $C_{2^n-1} \ltimes V_i$ to $\mathrm{AGL}_1(\mathbb{F}_{2^n})$ by

$$\kappa : \left(\sigma^j, U(x)\right) \mapsto \begin{bmatrix} g^{ij} & U(g^i) \\ 0 & 1 \end{bmatrix}$$

with $U(X) \in \mathbb{F}_2[X]$. By noting that σ acts on V_i by the multiplication of g, the map κ sends

$$\left(\sigma^j, U(x)\right)\left(\sigma^\ell, V(x)\right) = (\sigma^{j+\ell}, U(x) + x^j V(x))$$

to

$$\begin{bmatrix} g^{i(j+\ell)} & U(g^i) + g^{ij}V(g^i) \\ 0 & 1 \end{bmatrix}.$$

On the other hand, we compute

$$\begin{bmatrix} g^{ij} & U(g^i) \\ 0 & 1 \end{bmatrix}\begin{bmatrix} g^{i\ell} & V(g^i) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} g^{i(j+\ell)} & U(g^i) + g^{ij}V(g^i) \\ 0 & 1 \end{bmatrix}.$$

Therefore, κ is a homomorphism.

We see that $\left(\sigma^j, U(x)\right) \in \ker\kappa$ if and only if $g^{ij} = 1$ and $U(g^i) = 0$. The condition $g^{ij} = 1$ is equivalent to $j \equiv 0 (\mathrm{mod}\ 2^n - 1)$ since $(i, 2^n - 1) = 1$. The condition $U(g^i) = 1$ is equivalent to the minimal polynomial $\phi_i(X)$ of g^i divides $U(X)$. Therefore, the kernel consists of the trivial element only. Since the orders of both the groups are the same, the map κ is an isomorphism. ∎

We can now state our method of construction of F_{2^n}-extensions.

Theorem 3.3 *Recall that L is a cyclic extension of k of degree $2^n - 1$ and that ε_i is an idempotent defined by (3.1). Assume that $(i, 2^n - 1) = 1$. If $\theta \in \varepsilon_i\left(L^\times/(L^\times)^2\right)$ is nontrivial, then the Galois closure of $L\left(\sqrt{\theta}\right)$ over k is an F_{2^n}-extension over k.*

Proof We first note that $L^\times/(L^\times)^2$ is an $\mathbb{F}_2$-vector space on which $\mathrm{Gal}(L/k)$ acts and hence is an $\mathbb{F}_2[\mathrm{Gal}(L/k)]$-module. Let M be an irreducible $\mathbb{F}_2[\mathrm{Gal}(L/k)]$-submodule of $L^\times/(L^\times)^2$ generated by θ. By Lemma 3.1, the module M is of dimension n over $\mathbb{F}_2$. Let $(\theta = \theta_1, \dots, \theta_n)$ be a basis of M. Let K be the field generated by $\sqrt{\theta_i}$ $(i = 1, \dots, n)$, that is, $K = L\left(\sqrt{\theta_1}, \dots, \sqrt{\theta_n}\right)$.

We shall first show that K is a Galois extension over k. Let $\widetilde{\sigma}$ be an extension of $\sigma \in \mathrm{Gal}(L/k)$ to K. We compute

$$\left(\widetilde{\sigma}(\sqrt{\theta_i})\right)^2 = \widetilde{\sigma}(\theta_i) = \sigma(\theta_i).$$

Recalling that M is a multiplicative $\mathrm{Gal}(L/k)$-module, we have $\sqrt{\theta'} \in K$ for every element θ' of M. Moreover, in additive notation, there exists $A = [a_{ij}] \in \mathrm{GL}_n(\mathbb{F}_2)$

satisfying

$$\sigma(\theta_1,\ldots,\theta_n) = (\theta_1,\ldots,\theta_n)A. \tag{3.3}$$

In particular, we obtain $\widetilde{\sigma}(\sqrt{\theta_i}) = \pm\sqrt{\sigma(\theta_i)} \in K$. This shows that K/k is a Galois extension.

We have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(K/L) \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & \mathrm{Gal}(L/k) \arrow[r] & 1 \end{tikzcd} \qquad \text{(exact)}$$

induced from the restriction map. The Galois group $\mathrm{Gal}(L/k)$ acts on $\mathrm{Gal}(K/L)$: for $\gamma \in \mathrm{Gal}(K/L)$ and $\sigma \in \mathrm{Gal}(L/k)$, we choose an extension $\widetilde{\sigma}$ in $\mathrm{Gal}(K/k)$ and we define $\sigma \cdot \gamma = \widetilde{\sigma}\gamma\widetilde{\sigma}^{-1}$. This action is well defined because $\mathrm{Gal}(K/L)$ is abelian.

For $\sigma \in \mathrm{Gal}(L/k)$, we define $s(\sigma) \in \mathrm{Gal}(K/k)$ by

$$s(\sigma)(\sqrt{\theta_1},\ldots,\sqrt{\theta_n}) = (\sqrt{\theta_1},\ldots,\sqrt{\theta_n})A$$

with A defined in (3.3). It is easy to verify that this map s gives a splitting homomorphism and the above exact sequence splits.

By Kummer theory, there exists a bilinear nondegenerate pairing defined as

$$\langle\cdot,\cdot\rangle \; : \; \mathrm{Gal}(K/L) \times M \longrightarrow \mu_2 \longrightarrow \mathbb{F}_2, \quad (\gamma,\theta) \mapsto \frac{\gamma(\sqrt{\theta})}{\sqrt{\theta}}, \tag{3.4}$$

where the map $\mu_2 \longrightarrow \mathbb{F}_2$ is an isomorphism whose inverse map is $\mathbb{F}_2 \ni x \mapsto (-1)^x$. This yields an isomorphism

$$\mathrm{Gal}(K/L) \cong \mathrm{Hom}(M,\mathbb{F}_2), \quad \gamma \mapsto \langle\gamma,\theta\rangle. \tag{3.5}$$

Both the sides of (3.5) are $\mathrm{Gal}(L/k)$-modules. The action on the right-hand side is given by $\sigma(\theta \mapsto \langle\gamma,\theta\rangle) = (\theta \mapsto \langle\gamma,\sigma\theta\rangle)$.

We shall show that $\mathrm{Gal}(K/L)$ is an irreducible $\mathbb{F}_2[\mathrm{Gal}(L/k)]$-module isomorphic to $\varepsilon_j\mathbb{F}_2[\mathrm{Gal}(L/k)]$ for some integer j prime to 2^n-1. Then, from Lemma 3.2, $\mathrm{Gal}(K/k) \cong F_{2^n}$ follows. To do this end, we compute the action of $\sigma \in \mathrm{Gal}(L/k)$ on $\mathrm{Gal}(K/L)$ in terms of (3.3). In the above, we have shown that $\widetilde{\sigma}(\sqrt{\theta_i}) = \pm\sqrt{\sigma\theta_i}$, and thus we can define $e_i \in \mathbb{F}_2$ by

$$\widetilde{\sigma}(\sqrt{\theta_i}) = (-1)^{e_i}\sqrt{\sigma\theta_i}.$$

Using (3.3), we can compute further

$$\widetilde{\sigma}(\sqrt{\theta_i}) = (-1)^{e_i}\prod_{j=1}^{n}\sqrt{\theta_j}^{\,a_{ji}}.$$

By writing $A^{-1} = [b_{ij}]$, we have

$$\widetilde{\sigma}^{-1}\sqrt{\theta_i} = (-1)^{f_i}\sqrt{\sigma^{-1}\theta_i} = (-1)^{f_i}\prod_{j=1}^{n}\sqrt{\theta_j}^{\,b_{ji}}$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

with some $f_i \in \mathbb{F}_2$. The relation of e_i's and f_i's is derived by computing $\widetilde{\sigma}\widetilde{\sigma}^{-1}\left(\sqrt{\theta_i}\right) = \sqrt{\theta_i}$. In fact, the left-hand side is equal to

$$(-1)^{f_i}\widetilde{\sigma}\left(\prod_{j=1}^{n}\sqrt{\theta_j}^{b_{ji}}\right) = (-1)^{f_i}\prod_{j=1}^{n}(-1)^{e_j b_{ji}}\left(\prod_{k=1}^{n}\sqrt{\theta_j}^{a_{kj}}\right)^{b_{ji}} = (-1)^{f_i+\sum_{j=1}^{n} e_j b_{ji}}\sqrt{\theta_i}.$$

Hence, we obtain

$$f_i + \sum_{j=1}^{n} e_j b_{ji} = 0 \text{ for all } i = 1, \dots, n. \tag{3.6}$$

Now, let $(g_1, \dots, g_n)$ be the dual basis of $\mathrm{Gal}(K/L)$ with respect to the paring $\langle\cdot,\cdot\rangle$. We compute the action $\sigma \cdot g_i$ on $\sqrt{\theta_j}$:

$$\begin{aligned}(\sigma \cdot g_i)\left(\sqrt{\theta_j}\right) &= \widetilde{\sigma} g_i \widetilde{\sigma}^{-1}\left(\sqrt{\theta_j}\right) = \widetilde{\sigma} g_i\left((-1)^{f_j}\prod_{k=1}^{n}\sqrt{\theta_k}^{b_{kj}}\right)\\ &= (-1)^{f_j}\widetilde{\sigma}\left((-1)^{b_{ij}}\prod_{k=1}^{n}\sqrt{\theta_k}^{b_{kj}}\right) = (-1)^{f_j+b_{ij}}\prod_{k=1}^{n}\left(\widetilde{\sigma}\sqrt{\theta_k}\right)^{b_{kj}}\\ &= (-1)^{f_j+b_{ij}+\sum_{k=1}^{n} e_k b_{kj}}\sqrt{\theta_j}.\end{aligned}$$

Combining with (3.6), we have

$$(\sigma \cdot g_i)\left(\sqrt{\theta_j}\right) = (-1)^{b_{ij}}\sqrt{\theta_j}.$$

This means that σ acts on $\mathrm{Gal}(K/L)$ by A^{-1}. Therefore, $\mathrm{Gal}(K/L)$ is isomorphic to an irreducible module $\varepsilon_{-i}\mathbb{F}_2[\mathrm{Gal}(L/k)]$. Since $(-i, 2^n - 1) = 1$, we conclude $\mathrm{Gal}(K/k) \cong F_{2^n}$.

This completes the proof of Theorem 3.3. ■

Remark 3.4 Our proof shows that if σ acts on M by A as (3.3), then it acts on $\mathrm{Gal}(K/L)$ by A^{-1}. This argument does not depend on the assumption that $(i, 2^n - 1) = 1$. If we drop this assumption, then we obtain Galois extensions whose Galois groups are various semidirect products of $\mathrm{Gal}(L/k)$ and $\mathrm{Gal}(K/L)$ including the direct product. See [7, Section 6] for example.

The following corollary follows from the proof of Theorem 3.3.

Corollary 3.5 *With the same assumptions as in Theorem 3.3, the Galois closure of $L\left(\sqrt{\theta}\right)$ over k is $L\left(\sqrt{\sigma\theta} \mid \sigma \in \mathrm{Gal}(L/k)\right)$.*

The following corollary guarantees that there are infinitely many F_{2^n}-extensions containing L.

Corollary 3.6 *Let θ and θ' be nontrivial elements in $\varepsilon_i(L^\times/(L^\times)^2)$ for some i. The Galois closures of $L(\sqrt{\theta})$ and $L(\sqrt{\theta'})$ coincide if and only if the $\mathrm{Gal}(L/k)$-modules generated, respectively, by θ and θ' coincide.*

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

Proof This follows from the Kummer duality (3.4). ■

4 Identifying arithmetically equivalent fields

In the previous section, we have constructed F_{2^n}-extensions. In this section, we explain how to identify arithmetically equivalent fields inside the F_{2^n}-extensions.

We continue to use the notation used in the proof of Theorem 3.3. For convenience, we recall some of them. Let L/k be a cyclic extension of degree $2^n - 1$. We assume that i is an integer prime to $2^n - 1$ and consider an irreducible $\mathbb{F}_2[\mathrm{Gal}(L/k)]$-module M in $\varepsilon_i\left(L^\times/(L^\times)^2\right)$, where ε_i is the idempotent defined by (3.1). The module M is generated by θ and has a basis $(\theta = \theta_1, \ldots, \theta_n)$ over $\mathbb{F}_2$. We now fix a generator σ of $\mathrm{Gal}(L/k)$ and assume that σ acts on the above basis by (3.3). The Galois group $\mathrm{Gal}(K/L)$ is isomorphic to the dual group $\mathrm{Hom}(M, \mathbb{F}_2)$ of M (see (3.5)). We want to find quadratic extensions of $L(\sqrt{\theta})$ which are arithmetically equivalent but not conjugate. In Proposition 2.1, we have shown that all such quadratic extensions are arithmetically equivalent, and hence we only have to identify the conjugacy classes of these fields.

Definition 4.1 We denote by $\widetilde{\mathbb{F}_2^n}$ the quotient space of $\mathbb{F}_2^n$ by the subspace generated by $\boldsymbol{e}_1 = {}^t(1, 0, \ldots, 0)$. Namely, column vectors $\boldsymbol{e}$ and $\boldsymbol{f} \in \mathbb{F}_2^n$ are equal in $\widetilde{\mathbb{F}_2^n}$ if they coincide except for the first coordinate.

If $\tilde{\boldsymbol{v}} = {}^t(e_1, \ldots, e_n) \in \widetilde{\mathbb{F}_2^n}$, then a quadratic extension

$$Q(\tilde{\boldsymbol{v}}) = L\left(\sqrt{\theta}, \sqrt{\theta_2^{e_2} \cdots \theta_n^{e_n}}\right) \tag{4.1}$$

of $L\left(\sqrt{\theta}\right)$ is well defined and there is a one-to-one correspondence between such quadratic extensions and the set $\widetilde{\mathbb{F}_2^n} - \{\tilde{\boldsymbol{0}}\}$. The conjugate field of $Q(\tilde{\boldsymbol{v}})$ by σ is then given by

$$\sigma Q(\tilde{\boldsymbol{v}}) = L\left(\prod_{k=1}^{n} \sqrt{\theta_k^{a_{k1}}}, \prod_{k=1}^{n} \sqrt{\theta_k^{e_2 a_{k2} + \cdots + e_n a_{kn}}}\right)$$

with $A = [a_{ij}]$ in (3.3). The condition for $\sigma Q(\tilde{\boldsymbol{v}}) \supset L(\sqrt{\theta})$ is equivalent to that θ_1 coincides with either $\prod_{k=1}^{n} \theta_k^{e_2 a_{k2} + \cdots + e_n a_{kn}}$ or the product $\prod_{k=1}^{n} \theta_k^{a_{k1} + e_2 a_{k2} + \cdots + e_n a_{kn}}$ since $\prod_{k=1}^{n} \theta_k^{a_{k1}}$ does not coincide with θ_1. It is easy to observe that this condition holds if and only if $A\tilde{\boldsymbol{v}} = \boldsymbol{e}_1$. If $\tilde{\boldsymbol{v}}$ satisfies this condition, then $Q(\tilde{\boldsymbol{v}}) = Q(A^{-1}\boldsymbol{e}_1)$ is conjugate to $Q(A\boldsymbol{e}_1)$. Note that since $\mathrm{Gal}(L/k)$ acts transitively on $\widetilde{\mathbb{F}_2^n}$, for every element $\tilde{\boldsymbol{v}} \in \widetilde{\mathbb{F}_2^n}$, there exists an integer j such that $\tilde{\boldsymbol{v}} = A^j \boldsymbol{e}_1$.

In accordance with this observation, we define the following equivalence relation on $\widetilde{\mathbb{F}_2^n}$.

Definition 4.2 Let us fix σ as a generator of $\mathrm{Gal}(L/k)$, and let A be the matrix defined by (3.3). The elements $\tilde{\boldsymbol{v}} = A^i \boldsymbol{e}_1$ and $\tilde{\boldsymbol{f}} = A^j \boldsymbol{e}_1$ in $\widetilde{\mathbb{F}_2^n}$ are said to be equivalent if $i + j \equiv 0 (\mathrm{mod}\ 2^n - 1)$.

Using these definitions, we obtain the following proposition.

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

Proposition 4.1 *Let $\widetilde{\mathbb{F}_2^n}$ be the set defined by Definition 4.1. The map sending $\tilde{\boldsymbol{v}} \in \widetilde{\mathbb{F}_2^n}$ to $Q(\tilde{\boldsymbol{v}})$ as in (4.1) induces a one-to-one correspondence between the conjugacy classes over k of quadratic extensions over $L(\sqrt{\theta})$ and the equivalence classes of $\widetilde{\mathbb{F}_2^n} - \{\tilde{\mathbf{0}}\}$ by the equivalence relation in Definition 4.2.*

For explicit computation, it remains to give a basis of the irreducible module $M = \langle\theta\rangle$. We use the isomorphism

$$M \cong \mathbb{F}_2[X]/(\phi_i(X))$$

in (3.2) for that purpose. Recall that $\phi_i(X)$ is the minimal polynomial of g^i over $\mathbb{F}_2$, where g is a fixed generator of $\mathbb{F}_{2^n}^\times$, and that $\sigma \in \mathrm{Gal}(L/k)$ acts on the right-hand side by the multiplication by X. Thus, if we take $(1, X, \dots, X^{n-1})$ as a basis of $\mathbb{F}_2[X]/(\phi_i(X))$, then σ acts by the companion matrix of $\phi_i(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$:

$$\begin{bmatrix} 0 & 0 & & & & a_0 \\ 1 & 0 & & & & a_1 \\ 0 & 1 & \ddots & & & a_2 \\ \vdots & & \ddots & \ddots & & \vdots \\ & & & \ddots & 0 & a_{n-2} \\ 0 & & & \cdots & 1 & a_{n-1} \end{bmatrix}.$$

This matrix action is compatible if we take a basis $(\theta, \sigma\theta, \dots, \sigma^{n-1}\theta)$ for M.

To illustrate how the above method works, we give an explicit description for the case $n = 4$.

Proposition 4.2 *Let L be a cyclic extension of $\mathbb{Q}$ of degree 15 with Galois group generated by σ. If θ is a nontrivial element of $\varepsilon_1(L^\times/(L^\times)^2)$, then three fields*

$$L\left(\sqrt{\theta}, \sqrt{\sigma\theta}\right),\ L\left(\sqrt{\theta}, \sqrt{\sigma^2\theta}\right),\ L\left(\sqrt{\theta}, \sqrt{\sigma\theta\cdot\sigma^2\theta}\right)$$

are not conjugate but arithmetically equivalent.

Proof We consider an irreducible module $M = (\theta, \sigma\theta, \sigma^2\theta, \sigma^3\theta)$, which is isomorphic to $\mathbb{F}_2[X]/\phi_1(X) = \mathbb{F}_2[X]/(X^4 + X + 1)$. Hence, the action of σ is given by the companion matrix A of $\phi_1(X)$:

$$\sigma(\theta, \sigma(\theta), \sigma^2(\theta), \sigma^3(\theta)) = (\theta, \sigma(\theta), \sigma^2(\theta), \sigma^3(\theta)) \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $\boldsymbol{v}_i = A^i\boldsymbol{e}_1$ for $i = 0, \dots, 14$. If we denote the element in $\widetilde{\mathbb{F}_2^4}$ corresponding to $\boldsymbol{v}_i$ by $\tilde{\boldsymbol{v}}_i$, then the equivalence classes by Definition 4.1 are easily computed, and we have

$$\tilde{\boldsymbol{v}}_1 = \tilde{\boldsymbol{v}}_4,\ \tilde{\boldsymbol{v}}_2 = \tilde{\boldsymbol{v}}_8,\ \tilde{\boldsymbol{v}}_3 = \tilde{\boldsymbol{v}}_{14},\ \tilde{\boldsymbol{v}}_5 = \tilde{\boldsymbol{v}}_{10},\ \tilde{\boldsymbol{v}}_6 = \tilde{\boldsymbol{v}}_{13},\ \tilde{\boldsymbol{v}}_9 = \tilde{\boldsymbol{v}}_7,\ \tilde{\boldsymbol{v}}_{11} = \tilde{\boldsymbol{v}}_{12}.$$

We further connect them by the equivalence relation in Definition 4.2:

$$\tilde{\boldsymbol{v}}_i \sim \tilde{\boldsymbol{v}}_{15-i} \quad (i = 1, \dots, 7).$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

By combining these, it follows that the conjugacy classes of the quadratic extensions of $L(\sqrt{\theta})$ in K are

$$\begin{aligned}&\{Q(\tilde{\boldsymbol{v}}_1), Q(\tilde{\boldsymbol{v}}_3), Q(\tilde{\boldsymbol{v}}_{11})\},\\ &\{Q(\tilde{\boldsymbol{v}}_2), Q(\tilde{\boldsymbol{v}}_6), Q(\tilde{\boldsymbol{v}}_9)\},\\ &\{Q(\tilde{\boldsymbol{v}}_5)\}.\end{aligned}$$

Therefore, we can choose $Q(\tilde{\boldsymbol{v}}_1)$, $Q(\tilde{\boldsymbol{v}}_2)$, $Q(\tilde{\boldsymbol{v}}_5)$ as representatives of the conjugacy classes. These fields are nothing but ones in the statement of the proposition. ■

We give a numerical example of Proposition 4.2 using Magma [2].

Example 4.3 Let L be a unique cyclic extension of degree 15 inside the 31st cyclotomic field. A defining polynomial of L is

$$\begin{aligned}f(X) = X^{15} &- 31X^{14} + 434X^{13} - 3,627X^{12} + 20,150X^{11} - 78,430X^{10}\\ &+ 219,604X^9 - 447,051X^8 + 660,858X^7 - 700,910X^6 + 520,676X^5\\ &- 260,338X^4 + 82,212X^3 - 14,756X^2 + 1,240X - 31 \in \mathbb{Q}[X].\end{aligned}$$

Let α be a root of f and σ a generator of $\mathrm{Gal}(L/\mathbb{Q})$ sending α to $\alpha^3 - 6\alpha^2 + 9\alpha$. We have

$$\varepsilon_1 = \sigma + \sigma^2 + \sigma^3 + \sigma^4 + \sigma^6 + \sigma^8 + \sigma^9 + \sigma^{12}.$$

Unfortunately, we have $\varepsilon_1(\alpha) \in (L^\times)^2$, and we instead take $\theta = \varepsilon_1(\alpha + 1)$, which is nontrivial:

$$\begin{aligned}\theta = 1,918\alpha^{14} &- 55,941\alpha^{13} + 730,762\alpha^{12} - 5,642,195\alpha^{11} + 28,615,030\alpha^{10}\\ &- 100,198,470\alpha^9 + 247,832,148\alpha^8 - 435,429,135\alpha^7 + 538,848,977\alpha^6\\ &- 459,012,245\alpha^5 + 258,286,255\alpha^4 - 89,753,523\alpha^3 + 17,269,217\alpha^2\\ &- 1,514,740\alpha + 41,200.\end{aligned}$$

The Galois closure K of $L(\sqrt{\theta})$ is isomorphic to F_{2^4} as expected.

The arithmetically equivalent fields in Proposition 4.2 are generated, respectively, by

$$\begin{aligned}\sigma\theta =& - 1,868\alpha^{14} + 51,883\alpha^{13} - 644,123\alpha^{12} + 4,716,495\alpha^{11} - 22,632,746\alpha^{10}\\ &+ 74,787,369\alpha^9 - 174,015,255\alpha^8 + 286,515,188\alpha^7 - 330,720,046\alpha^6\\ &+ 261,327,388\alpha^5 - 135,654,656\alpha^4 + 43,411,399\alpha^3 - 7,829,444\alpha^2\\ &+ 707,661\alpha - 16,708,\\ \sigma^2\theta =& 568\alpha^{14} - 14,474\alpha^{13} + 159,857\alpha^{12} - 991,986\alpha^{11} + 3,704,900\alpha^{10}\\ &- 7,937,152\alpha^9 + 6,068,083\alpha^8 + 15,337,953\alpha^7 - 53,985,594\alpha^6\\ &+ 78,016,586\alpha^5 - 62,566,399\alpha^4 + 27,793,973\alpha^3 - 6,084,932\alpha^2\\ &+ 495,906\alpha + 900,\end{aligned}$$

https://doi.org/10.4153/S0008439522000388 Published online by Cambridge University Press

$$\begin{aligned}\sigma\theta\cdot\sigma^2\theta = &-2,171,688\alpha^{14}+67,084,221\alpha^{13}-934,645,093\alpha^{12}+7,750,575,584\alpha^{11}\\ &-42,508,235,392\alpha^{10}+162,029,379,062\alpha^{9}-438,947,076,273\alpha^{8}\\ &+849,307,812,685\alpha^{7}-1,162,572,370,875\alpha^{6}+1,098,352,512,421\alpha^{5}\\ &-685,146,475,599\alpha^{4}+262,216,335,852\alpha^{3}-54,652,878,964\alpha^{2}\\ &+5,143,605,707\alpha-112,645,567.\end{aligned}$$

The three fields in Proposition 4.2 share the same Dedekind zeta function

$$\begin{aligned}\zeta(s) = &\frac{1}{1^s}+\frac{4}{31^s}+\frac{3}{32^s}+\frac{12}{61^s}+\frac{20}{125^s}+\frac{60}{311^s}+\frac{12}{373^s}+\frac{12}{433^s}\\ &+\frac{12}{557^s}+\frac{12}{619^s}+\frac{12}{683^s}+\frac{12}{743^s}+\frac{12}{929^s}+\frac{10}{961^s}+\frac{12}{991^s}+\frac{12}{992^s}+\cdots.\end{aligned}$$

The referee pointed out that if we take the minimal polynomial of $2\cos\left(\frac{2\pi}{31}\right)$ as f, then we can obtain elements with smaller coefficients.

Acknowledgment The author would like to thank the anonymous referee for his/her careful reading of the manuscript and many invaluable comments.

References

[1] M. Aigner, *A course in enumeration*, Graduate Texts in Mathematics, 238, Springer, Berlin, 2007.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: the user language*, J. Symb. Comput. 24 (1997), nos. 3–4, 235–265, Computational algebra and number theory (London, 1993).

[3] M. Hall Jr., *Combinatorial theory*. 2nd ed., Wiley-Interscience Series in Discrete Mathematics, Wiley, New York, 1986.

[4] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, 134, Springer, Berlin and New York, 1967.

[5] I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, 69, Academic Press, New York and London, 1976.

[6] Y. Katayama and M. Kida, *Coincidence of L-functions*. Acta Arith., to appear.

[7] M. Kida, *On metacyclic extensions*. J. Théor. Nombres Bordeaux 24(2012), no. 2, 339–353.

[8] N. Klingen, *Arithmetical similarities*, Oxford Mathematical Monographs, Clarendon Press and Oxford University Press, New York, 1998.

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

Department of Mathematics, Faculty of Science Division I, Tokyo University of Science, 1-3 Kagurazaka Shinjuku, Tokyo 162-8601, Japan
e-mail: kida@rs.tus.ac.jp