Canad. J. Math. Vol. 75 (3), 2023 pp. 804–827
http://dx.doi.org/10.4153/S0008414X22000165

Galois module structure of square power classes for biquadratic extensions

Frank Chemotti, Ján Mináč, Andrew Schultz and John Swallow

Abstract. For a Galois extension K/F with $\mathrm{char}(K) \neq 2$ and $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, we determine the $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-module structure of $K^\times/K^{\times 2}$. Although there are an infinite number of (pairwise nonisomorphic) indecomposable $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$-modules, our decomposition includes at most nine indecomposable types. This paper marks the first time that the Galois module structure of power classes of a field has been fully determined when the modular representation theory allows for an infinite number of indecomposable types.

1 Introduction

1.1 Background and motivation

Let K be a field, and write ξ_p for a primitive pth root of unity. We write K_{sep} for a separable closure of K, and $K(p)$ for the maximal p-extension within K_{sep}. Each of these extensions is Galois. The absolute Galois group of K is the group $G_K := \mathrm{Gal}(K_{\mathrm{sep}}/K)$. The group $G_K(p) := \mathrm{Gal}(K(p)/K)$ is the maximal pro-p quotient of G_K. For convenience, we will call $G_K(p)$ the *absolute p-Galois group* of K. One of the major open problems in Galois theory is to determine those profinite groups G for which there exists some field K with $G_K \simeq G$, i.e., to distinguish absolute Galois groups within the class of profinite groups. This problem is very difficult. The analogous question for pro-p groups—to distinguish absolute p-Galois groups within the class of pro-p groups—is also unsolved and extremely difficult.

How does one look for those properties that distinguish absolute p-Galois groups from the broader class of pro-p groups? To motivate the perspective pursued in this paper, note that since $G_K(p)$ is a pro-p group, it is natural to study it recursively through its Frattini subgroup and its quotient. This quotient is the maximal elementary p-abelian quotient of $G_K(p)$, which by Kummer theory (assuming $\xi_p \in K$) corresponds to $J(K) := K^\times/K^{\times p}$. In the case that K is itself a Galois extension of a field

Received by the editors September 1, 2021; revised April 15, 2022; accepted April 19, 2022.
Published online on Cambridge Core April 25, 2022.
The second author is partially supported by the Natural Sciences and Engineering Research Council of Canada grant R0370A01. He also gratefully acknowledges the Faculty of Science Distinguished Research Professorship, Western Science, in years 2004/2005 and 2020/2021. The third author is partially supported by 2017–2019 Wellesley College Faculty Awards. The fourth author was supported in part by the National Security Agency grant MDA904-02-1-0061.
AMS subject classification: **12F10**, 16D70.
Keywords: Biquadratic extension, Galois module, Hilbert 90, pro-p groups, absolute Galois groups, Klein 4-group.

F, one then has a natural action of $\mathrm{Gal}(K/F)$ on $J(K)$. (Throughout the remainder of this discussion, we will assume that $\mathrm{Gal}(K/F)$ is a p-group, just to stay firmly planted in the context of p-groups.) One field-theoretic lens for studying $G_K(p)$, therefore, is to determine the structure of $J(K)$ as a module over $\mathbb{F}_p[\mathrm{Gal}(K/F)]$. It is worth noting that the submodules of $J(K)$ are in bijection with the elementary p-abelian extensions of K that are additionally Galois over F (see [31]), again assuming $\xi_p \in K$.

Given that the modular representation theory of $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ is most tractable when $\mathrm{Gal}(K/F)$ is cyclic, this is a natural place to begin. Some early work by Borevič and Fadeev (see [7, 12]) examined the module structure of $J(K)$ when K is a local field and $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$ using local class field theory. Subsequently, Mináč and Swallow [26] showed that the module $J(K)$ can be computed when $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$ assuming only $\xi_p \in K$ and without such heavy machinery.

The surprise from this result is twofold. First, despite the fact that the field K is completely general, the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module $J(K)$ is far more stratified than a "random" $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-module: whereas a general $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-module can have summands drawn from any one of p possible isomorphism types, the decomposition of $J(K)$ as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module involves at most three isomorphism classes of indecomposable summands (free cyclic modules, trivial cyclic modules, and at most one cyclic module of dimension 2). The second surprise comes from the proof of the result itself. Although this decomposition requires a lot of careful work, the machinery needed for the proof is actually quite elementary. Indeed, the key theoretical tool in the proof is Hilbert's Satz 90.

The benefit of an elementary approach to the decomposition of $J(K)$ when $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\xi_p \in K$ is not just that it lets one compute this module for arbitrary K, but also that it provides a road map for how one might generalize this decomposition to a broader class of Galois modules. Indeed, generalizations of this type have been carried out in a variety of contexts. In [23], three of the authors gave the decomposition of $J(K)$ whenever $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Looking past power classes, observe that when $i = 1$ and $\xi_p \in K$, we have $H^i(G_K(p), \mathbb{F}_p) \simeq K^\times/K^{\times p}$ as Galois modules, so higher cohomology groups provide a new family of Galois modules to investigate. Using the connection between Milnor K-theory and Galois cohomology—together with the generalization of Hilbert 90 to this context—two of the authors and Lemire gave a decomposition of the Galois cohomology groups $H^i(G_K(p), \mathbb{F}_p)$ in [20] under the assumption that $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\xi_p \in K$. Some partial results for the structure of $H^i(G_K(p), \mathbb{F}_p)$ when $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$ are given in [19]. Generalizations to the case where K is characteristic p (but $\mathrm{Gal}(K/F)$ is still assumed to be a cyclic p-group) have also been explored in [5, 6, 25, 29].

As with the original decomposition of $J(K)$ in [26], these subsequent module decompositions contain far fewer isomorphism classes of indecomposables than one might expect *a priori*. These stratified decompositions have, in turn, been translated into properties that distinguish absolute p-Galois groups within the larger class of pro-p groups. For example, using the structure of $J(K)$, a variety of automatic realization and realization multiplicity results have been proved (see [5, 8, 24, 27, 29]). The module structure for cohomology groups computed in [20] was used in [4] to find a number of pro-p groups that are not absolute p-Galois groups.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

It would be natural to assume that the previous module computations are possible because the modular representation theory for the group ring $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ is simple when $\mathrm{Gal}(K/F)$ is cyclic—namely, in this case, there are $|\mathrm{Gal}(K/F)|$ isomorphism classes of indecomposables, and each of them is cyclic. In contrast, if G is a noncyclic elementary p-abelian group, then there are infinitely many isomorphism classes of indecomposable $\mathbb{F}_p[G]$-modules (and often it is impossible to give a full classification of indecomposables). There has been some work which provides partial information about Galois modules in these more complicated settings, recovering information about the Socle series or arguing that the modules are constant Jordan type in special cases [1, 11, 28]. However, these modules were not determined completely.

In this paper, we provide a decomposition for $J(K)$ as an $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-module when $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, without any restriction on K other than $\mathrm{char}(K) \neq 2$. The decomposition follows the two themes that have arisen in the context of cyclic Galois groups: the module structure is far more stratified than one would expect for a general module (across all fields K, the summands are drawn from at most nine indecomposable types), and the decomposition can be determined using relatively concrete techniques and the assistance of Hilbert 90 (see [10] for a discussion on how one interprets Hilbert 90 for biquadratic extensions). Undoubtedly, this stratified decomposition—both the appearance of some summand types and the exclusion of others—can be translated into new and exciting group-theoretic properties of absolute 2-Galois groups. The authors are currently looking into such results.

A decomposition of $J(K)$ when $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ was completed by the first, second, and fourth authors in 2005 using more technical machinery. (This previous work is not publicly available, but we believe that the results and exposition in the current article supersede and enhance the 2005 work.) A deeper dive into the module from this perspective was explored in [13] under the joint supervision of Minač and Swallow. The impetus for revisiting this problem using more ubiquitous tools was to give greater insight into how decompositions for $J(K)$ (and its ilk) could be carried out when $\mathrm{Gal}(K/F)$ is some other elementary p-abelian group. This approach has already met with success: it has allowed us to exclude one summand type that appeared in the original decomposition from 2005, and it inspired the recent decomposition of the parameterizing space of elementary p-abelian extensions of K as a module over $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ whenever $G_F(p)$ is a free, finitely generated pro-p group and $\mathrm{Gal}(K/F)$ is *any* finite p-group (see the remark after Theorem 1.1). We are hopeful that the techniques we develop here can inspire the next steps toward investigations of a broader class of elementary p-abelian Galois modules.

1.2 Statement of the main result

We first set terminology that will hold for the rest of the paper. Suppose that F is a field with $\mathrm{char}(F) \neq 2$ and that K/F is an extension with $G := \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let $a_1, a_2 \in F$ be given so that $K = F(\sqrt{a_1}, \sqrt{a_2})$, and let $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ be their duals; that is, we have $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$. For $i \in \{1, 2\}$, we define $K_i = F(\sqrt{a_i})$. Write H_i for the subgroup of $\mathrm{Gal}(K/F)$ which fixes elements in K_i, and $\overline{G_i}$ for the corresponding quotient group: $\overline{G_i} := \mathrm{Gal}(K_i/F) = \{\overline{\mathrm{id}}, \overline{\sigma_i}\}$. In the same spirit, write $K_3 = F(\sqrt{a_1a_2})$, denote the subgroup of $\mathrm{Gal}(K/F)$ which fixes K_3 as H_3, and use

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

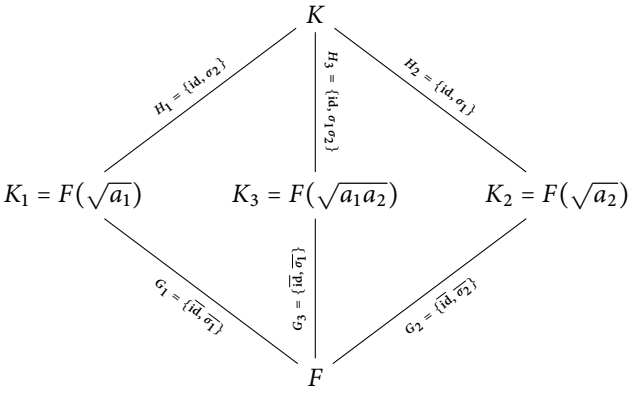


Figure 1: The lattice of fields for K/F, with corresponding Galois groups.

$\overline{G_3}$ for the corresponding quotient $G/H_3 = \mathrm{Gal}(K_3/F)$. To round out the notation, let $H_0 = \{\mathrm{id}\}$ (the elements which fix the extension K/F) and $H_4 = \mathrm{Gal}(K/F)$ (the elements which fix the extension F/F), and use $\overline{G_0}$ and $\overline{G_4}$ for their quotients. (See Figure 1.)

In our result below, we use Ω^{-n} and Ω^n to denote certain indecomposable modules of dimension $2n+1$; more information on these modules can be found in Section 2.

Theorem 1.1 *Suppose that* $\mathrm{char}(K) \neq 2$ *and that* $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. *Let* $J(K) = K^\times/K^{\times 2}$. *Then, as an* $\mathbb{F}_2[\mathrm{Gal}(K/F)]$*-module, we have*

$$J(K) \simeq X \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 \oplus Z_1 \oplus Z_2,$$

where

- X *is isomorphic to one of the following:* $\{0\}, \mathbb{F}_2, \mathbb{F}_2 \oplus \mathbb{F}_2, \Omega^{-1}, \Omega^{-2}$, *or* $\Omega^{-1} \oplus \Omega^{-1}$;
- *for each* $i \in \{0,1,2,3,4\}$, *the summand* Y_i *is a direct sum of modules isomorphic to* $\mathbb{F}_2[\overline{G_i}]$; *and*
- *for each* $i \in \{1,2\}$, *the summand* Z_i *is a direct sum of modules isomorphic to* Ω^i.

Remark 1.2 When $\mathrm{char}(K) = 2$, elementary 2-abelian extensions of K are parameterized by $\mathbb{F}_2$-subspaces of $K/\wp K$, where $\wp K = \{k^2 - k : k \in K\}$. It is therefore natural to ask whether $K/\wp(K)$ can be decomposed as an $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-module as well. The answer is a resounding "yes." Indeed, when p is any prime number and $\mathrm{char}(K) = p$, the thesis [14] gives the structure of $K/\{k^p - k : k \in K\}$ as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module whenever $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. This decomposition reveals that the only non-free summand is isomorphic to $\Omega^{-2}_{\mathrm{Gal}(K/F)}$. This result is extended considerably in the forthcoming paper [15]: for any prime p and any Galois extension K/F so that $\mathrm{Gal}(K/F)$ is a finite p-group, if $G_F(p)$ is a free pro-p group that is finitely generated, then the parameterizing space of elementary p-abelian extensions of K decomposes into a free summand and a single summand isomorphic to $\Omega^{-2}_{\mathrm{Gal}(K/F)}$.

Theorem 1.1 helps give new insight into the question of what distinguishes absolute 2-Galois groups from the broader class of pro-2 groups. By equivariant Kummer

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

theory, we know that $J(K)$ is dual to the maximal elementary 2-abelian quotient of $G_K(2)$. Theorem 1.1 (together with the main result of [14] to address the characteristic 2 case) tells us that whenever G is the absolute 2-Galois group of a field F, then for every continuous surjection $G \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the maximal elementary p-abelian quotient of the kernel of this surjection has a particular module structure attached to it.

Alternatively, one could attempt to use this result to uncover specific information about embedding problems over $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ extensions. To do this, one needs a dictionary that translates module- and field-theoretic information associated to submodules of $J(K)$ into structural properties of the Galois groups to which they correspond. Such a dictionary already exists in the case where $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/p\mathbb{Z}$ (see [29, 31]) and has been used to great effect to show how the Galois module structure of $J(K)$ in this case reveals distinguishing properties of absolute p-Galois groups (e.g., automatic realization results that one would not expect from group theory alone; see [24, 27, 29]).

Indeed, such a dictionary in the biquadratic case can be used to calculate all information about $J(K)$ simultaneously: for a given biquadratic extension K/F, one creates a pro-2 extension L/F by defining $L = K(\sqrt{\gamma} : \gamma \in J(K))$, and the aforementioned dictionary would allow us to compute $\mathrm{Gal}(L/F)$. This would give an important invariant attached to any biquadratic extension of F, and exhibit some critical distinctions between absolute 2-Galois groups and the larger class of pro-2 groups. The authors of this manuscript are already working to provide this dictionary, an effort that should produce yet more explicit manifestations for the "specialness" of absolute 2-Galois groups.

1.3 Outline of the paper

In Section 2, we review some basic facts concerning modules over $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$. Section 3 is devoted to producing a "large" module whose fixed part is the "obvious" component $[F^\times]$ within $J(K)^G$; the key is to give a filtration of $[F^\times]$ that is sensitive to image subspaces coming from particular elements of $\mathbb{F}_2[G]$. Section 4 aims to find a module whose fixed part spans a complement to $[F^\times]$ in $J(K)^G$. This requires a deeper understanding of how $J(K)^G$ behaves under the norm maps associated to the intermediate extensions K/K_i (for $i \in \{1, 2, 3\}$). The proof of Lemma 4.6 gives our first appearance of a Hilbert 90 result for biquadratic extensions. Section 5 has another result related to Hilbert 90 for biquadratic extensions (Lemma 5.1), as well as the proof of Theorem 1.1. In Section 6, we discuss the realizability of some of the possibilities for the X summand in terms of the solvability (or nonsolvability) of particular embedding problems.

2 A primer in diagrammatic thinking in module theory

We will use G to denote the Klein 4-group with generators σ_1 and σ_2. When M is an $\mathbb{F}_2[G]$-module, we assume that M's structure is multiplicative, so that the module action is written exponentially. Despite this, if U, V are submodules of a larger

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

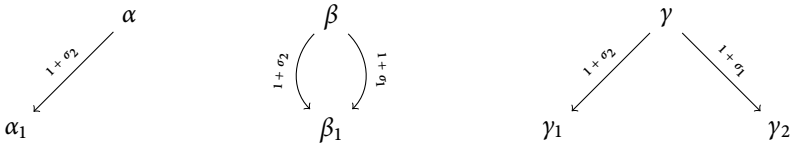


Figure 2: A sampling of linear equations. On the left, we have the relation $\alpha^{1+\sigma_2} = \alpha_1$; in the middle, we have the simultaneous equations in β and β_1 given by $\beta^{1+\sigma_1} = \beta^{1+\sigma_2} = \beta_1$; and on the right, we have the simultaneous equations in $\gamma, \gamma_1, \gamma_2$ given by $\gamma^{1+\sigma_2} = \gamma_1$ and $\gamma^{1+\sigma_1} = \gamma_2$.

$\mathbb{F}_2[G]$-module W, we will still write $U + V$ for the set $\{uv : u \in U, v \in V\}$, and we will use $U \oplus V$ to indicate this set when $U \cap V$ is trivial.

Throughout this paper, we will be considering the solvability of certain systems of equations within various $\mathbb{F}_2[G]$-modules. Although one could of course write these systems out, it will often be convenient to have graphical representations for the equations. We adopt the convention that an arrow between elements denotes that one is the image of another through some given element of $F_2[G]$, with the direction of the arrow indicating the acting element from $\mathbb{F}_2[G]$. If the arrow points down and to the left, this indicates that the bottom element is the image of the upper element under $1 + \sigma_2$, and likewise if the arrow points down and to the right, this means the lower element is the image of the upper element under $1 + \sigma_1$. In the event that the action of $1 + \sigma_1$ and $1 + \sigma_2$ is the same on a given element, then we write the image immediately below, and use two bent arrows to signify the equality of the two actions. Figure 2 gives some basic examples.

Since these diagrams represent simultaneous linear equations in the module, we will say that a solution to a system of equations is a solution to the corresponding diagram; if we have some fixed values for particular parameters in a system of equations, and there exist values for the remaining parameters so that the underlying system is solved, then we will say that the diagram is solvable for those (original) fixed values. For example, to say that the diagram on the left side of Figure 2 is solvable for some particular α_1 is equivalent to saying that α_1 is in the image of $1 + \sigma_1$.

Our decomposition will not require us to have a classification of indecomposable $\mathbb{F}_2[G]$-modules, but for the reader's benefit, we review some basic information about these modules. For a full treatment, the reader can consult [3, Theorem 4.3.3]. There are seven ideals in the ring $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$, and hence six cyclic, nontrivial indecomposable submodule classes. Aside from the even-dimensional cyclic modules, there are also families of indecomposable even-dimensional $\mathbb{F}_2[G]$-modules that correspond to certain rational canonical form matrices. These will not appear in our decomposition. There are also odd-dimensional indecomposable $\mathbb{F}_2[G]$-modules: for each odd number $2n + 1$ with $n \geq 1$, there are two irreducible $\mathbb{F}_2[G]$-modules of dimension n, denoted Ω^n and Ω^{-n}. As it happens, our decomposition of $J(K)$ will only require the cyclic modules we have already introduced together with $\Omega^1, \Omega^2, \Omega^{-1}$, and Ω^{-2}. We will need formal definitions for these latter modules, but there is no additional cost to define Ω^n and Ω^{-n} in general. Using our depiction scheme, these modules are shown in Figure 3.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

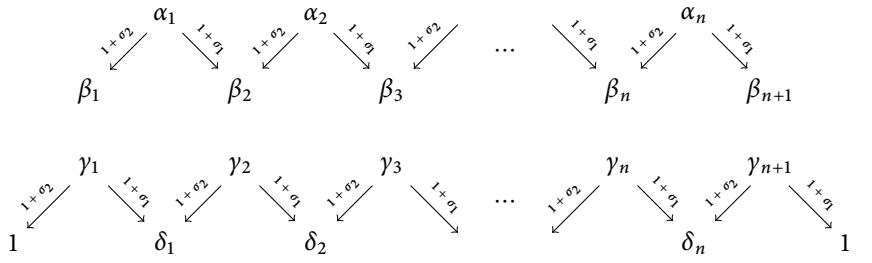


Figure 3: The two indecomposable $\mathbb{F}_2[G]$-modules of odd dimension $2n+1$: Ω^{-n} (depicted above) and Ω^n (depicted below). Although it is not explicit in the diagram, each of the β_i and δ_i is fixed by the action of G.

One key fact we will use about $\mathbb{F}_2[G]$-module is that we can detect independence of two $\mathbb{F}_2[G]$-modules by examining the independence of their fixed parts. We follow the standard convention of writing M^G for the fixed submodule of an $\mathbb{F}_2[G]$-module M.

Lemma 2.1 *Suppose that M and N are submodules of a larger $\mathbb{F}_2[G]$-module W. Then $M \cap N = \{1\}$ if and only if $M^G \cap N^G = \{1\}$.*

Proof Of course, if $M \cap N = \{1\}$, then $M^G \cap N^G = \{1\}$ as well. Suppose, then, that $M^G \cap N^G = \{1\}$, and let $w \in M \cap N$ be given. If w is nontrivial, then $\langle w \rangle$ is isomorphic to precisely one of the following: $\mathbb{F}_2$, $\mathbb{F}_2[\overline{G_1}]$, $\mathbb{F}_2[\overline{G_2}]$, $\mathbb{F}_2[\overline{G_3}]$, Ω^{-1}, or $\mathbb{F}_2[G]$. In the first case, we have $w \in W^G$, and so $w \in M^G \cap N^G = \{1\}$; this is a contraction. If either $\langle w \rangle \simeq \mathbb{F}_2[\overline{G_1}]$, $\langle w \rangle \simeq \mathbb{F}_2[\overline{G_3}]$, or $\langle w \rangle \simeq \Omega^{-1}$, then $w^{1+\sigma_1}$ is a nontrivial element in W^G; but this again leads to a contradiction, since then we again have $w^{1+\sigma_1} \in M^G \cap N^G = \{1\}$. If $\langle w \rangle \simeq \mathbb{F}_2[\overline{G_2}]$, then $w^{1+\sigma_2}$ is the nontrivial element in W^G, which leads to a contradiction, and if $\langle w \rangle \simeq \mathbb{F}_2[G]$, then the contradictory nontrivial element of W^G is $w^{(1+\sigma_1)(1+\sigma_2)}$. ∎

3 A maximal submodule with fixed part $[F^\times]$

In Section 2, we saw that fixed submodules play an important role in determining independence among $\mathbb{F}_2[G]$-modules. Of course, the most natural fixed submodule of $J(K)$ is $[F^\times]$. Our objective in this section will be to find a "sufficiently large" submodule $\widehat{J}$ of $J(K)$ for which $\widehat{J}^G = [F^\times]$. For the purposes of the decomposition that we are building, being "sufficiently large" will mean that $\widehat{J}$ contains solutions to certain systems of equations, assuming such equations have solutions within the full module $J(K)$.

In a certain sense, we are most interested in finding free summands—by which we mean free over $\mathbb{F}_2[\overline{G_i}]$ for some $i \in \{0,1,2,3,4\}$—with the general philosophy that larger submodules are preferable. Hence, primary preference goes to free (cyclic) $\mathbb{F}_2[G]$-modules, and secondary preference goes to free (cyclic) $\mathbb{F}_2[\overline{G_i}]$-modules for $i \in \{1,2,3\}$; for concreteness, we give preference to $i=1$ over $i=2$, and $i=2$ over $i=3$. We finish with free $\mathbb{F}_2[\overline{G_4}]$-modules (i.e., trivial modules).

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

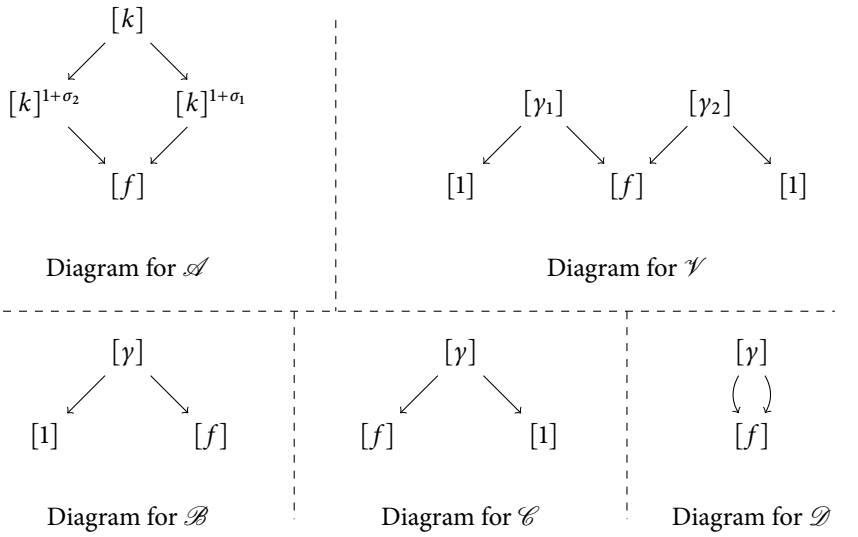
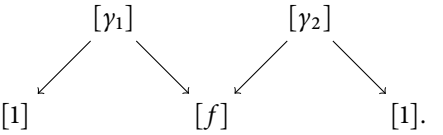


Figure 4: Diagrams that represent the various systems of equations that are solvable in order for $[f]$ to be an element of the subspaces $\mathscr{A}, \mathscr{V}, \mathscr{B}, \mathscr{C}$, or $\mathscr{D}$.

The issue in pursuing this agenda is that there are potential interrelations between these free modules. For example, suppose a free cyclic $\mathbb{F}_2[\overline{G_1}]$-module $\langle[\gamma_1]\rangle$ and a free cyclic $\mathbb{F}_2[\overline{G_2}]$-module $\langle[\gamma_2]\rangle$ share the same fixed submodule $\langle[f]\rangle$. This means that $[f], [\gamma_1]$, and $[\gamma_2]$ satisfy the system of equations



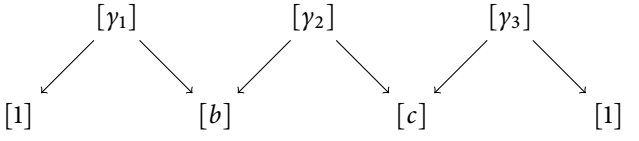
Hence, in our pursuit of free submodules, we are obliged to look for solutions to this type of system and ensure our decomposition of $[F^\times]$ captures these elements.

With all this in mind, let us move toward statements that are more precise. In Figure 4, we introduce five subspaces of $[F^\times]$ that capture the ideas we alluded to in the previous paragraphs. We denote these spaces $\mathscr{A}, \mathscr{V}, \mathscr{B}, \mathscr{C}$, and $\mathscr{D}$. For $\mathscr{M} \in \{\mathscr{A}, \mathscr{V}, \mathscr{B}, \mathscr{C}, \mathscr{D}\}$, the space $\mathscr{M}$ is the set of all $[f] \in [F^\times]$ for which the corresponding diagram from Figure 4 is solvable for $[f]$. For example, an element $[f] \in [F^\times]$ is an element of $\mathscr{A}$ if and only if $[f] \in [N_{K/F}(K^\times)]$ (since $N_{K/F}$ is given by applying $(1+\sigma_1)(1+\sigma_2)$).

It is readily apparent that $\mathscr{A} \subseteq \mathscr{V}$, and furthermore that $\mathscr{V}$ is a subspace of both $\mathscr{B}$ and $\mathscr{C}$. We just observed that $\mathscr{B} \cap \mathscr{C} = \mathscr{V}$. Continuing in the theme of being careful about interrelations that exist between these subspaces, the following lemma considers how elements of $\mathscr{D}$ are related to elements from $\mathscr{B} + \mathscr{C}$.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

Lemma 3.1 *Let $\mathscr{B}, \mathscr{C}$, and $\mathscr{D}$ be defined as in Figure 4. Then $[b][c] \in (\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$ if and only if*



(3.1)

is solvable for some $[\gamma_1], [\gamma_2], [\gamma_3] \in J(K)$.

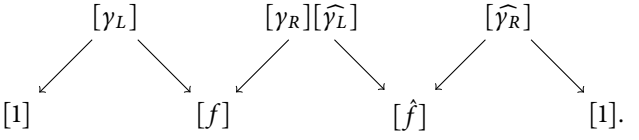
Proof Suppose first that equation (3.1) holds. From this, we see that

$$([\gamma_1][\gamma_2][\gamma_3])^{1+\sigma_2} = [1][b][c],$$
$$([\gamma_1][\gamma_2][\gamma_3])^{1+\sigma_1} = [b][c][1].$$

Hence, $[b][c] \in (\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$.

For the other direction, suppose there exists $[\gamma] \in J(K)$ so that the diagram for $\mathscr{D}$ holds with $[\gamma]$ and $[f] = [b][c]$. Since $[b] \in \mathscr{B}$ and $[c] \in \mathscr{C}$, we also have elements $[\gamma_L], [\gamma_R] \in J(K)$ so that $[\gamma_L]$ and $[b]$ satisfy the diagram for $\mathscr{B}$, and $[\gamma_R]$ and $[c]$ satisfy the diagram for $\mathscr{C}$. From these relations, we find that equation (3.1) is satisfied with $[\gamma_1] = [\gamma_L]$, $[\gamma_2] = [\gamma_L][\gamma][\gamma_R]$, and $[\gamma_3] = [\gamma_R]$. ∎

Notice that if $[f]$ and $[\hat{f}]$ are elements of $\mathscr{V}$ (with corresponding elements $[\gamma_L], [\gamma_R]$ solving the diagram with $[f]$, and $[\widehat{\gamma_L}], [\widehat{\gamma_R}]$ solving the diagram for $[\hat{f}]$), then equation (3.1) is solvable for $[b] = [f]$ and $[c] = [\hat{f}]$:



Hence, we will be particularly interested in understanding solutions to equation (3.1) that come from outside $\mathscr{V}$. The following lemma characterizes such solutions.

Lemma 3.2 *Suppose that B is a complement to $\mathscr{V}$ within $\mathscr{B}$, and that C is a complement to $\mathscr{V}$ within $\mathscr{C}$. Define subspaces B_W of B and C_W of C by*

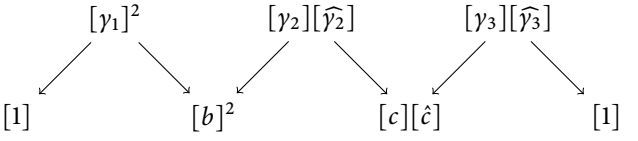
$$B_W = \{[b] \in B : \exists [c] \in C \text{ so that equation (3.1) is solvable}\},$$
$$C_W = \{[c] \in C : \exists [b] \in B \text{ so that equation (3.1) is solvable}\}.$$

Then there exists an $\mathbb{F}_2$-linear bijection $\phi_W : B_W \to C_W$ which takes each $[b] \in B_W$ to the unique $[c] \in C_W$ for which equation (3.1) is solvable for $[b]$ and $[c]$.

Proof That B_W and C_W are subspaces follows since equation (3.1) is linear. Now, we claim that, for each $[b] \in B_W$, there exists a unique $[c] \in C_W$ for which the equations represented by equation (3.1) are solvable. Suppose instead we had some $[b] \in B_W$ so that there exist $[c], [\hat{c}] \in C_W$ which make equation (3.1) solvable; we will write $[\gamma_1], [\gamma_2], [\gamma_3]$ for the additional terms that solve the system with $[b]$ and $[c]$, and

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

we will write $[\gamma_1], [\widehat{\gamma_2}], [\widehat{\gamma_3}]$ for the additional terms that solve the system with $[b]$ and $[\hat{c}]$. By multiplying the two systems, we are left with



and so we see that $[c][\hat{c}] \in \mathscr{V}$. However, since $[c]$ and $[\hat{c}]$ are contained in a complement C of $\mathscr{V}$ within $\mathscr{C}$, this implies $[c][\hat{c}] = [1]$. Hence, $[c] = [\hat{c}]$.

The same argument, of course, shows that, for a given $[c] \in C_W$, there exists a unique $[b] \in B_W$ for which equation (3.1) is solvable. We define ϕ_W as the function which associates to each $[b] \in B_W$ its corresponding $[c] \in C_W$. The fact that the equations represented by equation (3.1) are linear implies that ϕ_W is linear as well, and hence an isomorphism of $\mathbb{F}_2$-spaces. ∎

We are now prepared to state and prove the main result in this section.

Theorem 3.3 *There exists a submodule $\widehat{J}$ of $J(K)$ so that $\widehat{J}^G = [F^\times]$, and for which*

$$\widehat{J} \simeq Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C \oplus Y_D \oplus Y_F,$$

where

- *Y_A is a direct sum of submodules isomorphic to $\mathbb{F}_2[G]$;*
- *Y_V is a direct sum of submodules isomorphic to Ω^1;*
- *Y_W is a direct sum of submodules isomorphic to Ω^2;*
- *Y_B is a direct sum of submodules isomorphic to $\mathbb{F}_2[\overline{G_1}]$;*
- *Y_C is a direct sum of submodules isomorphic to $\mathbb{F}_2[\overline{G_2}]$;*
- *Y_D is a direct sum of submodules isomorphic to $\mathbb{F}_2[\overline{G_3}]$; and*
- *Y_F is a direct sum of submodules isomorphic to $\mathbb{F}_2$.*

Proof Choose $\mathcal{A}$ to be an $\mathbb{F}_2$-basis for $\mathscr{A}$. By the definition of $\mathscr{A}$, for each $[f] \in \mathcal{A}$, there exists some $[\gamma_f] \in [K^\times]$ so that $[N_{K/F}(\gamma_f)] = [f]$. We define $M_{[f]} := \langle [\gamma_f] \rangle$, and observe that $M_{[f]} \simeq \mathbb{F}_2[G]$ and $M_{[f]}^G = \langle [f] \rangle$. Let $Y_A = \sum_{[f] \in \mathcal{A}} M_{[f]}$. Observe that $Y_A = \bigoplus_{[f] \in \mathcal{A}} M_{[f]}$ by Lemma 2.1, and that $Y_A^G = \bigoplus_{[f] \in \mathcal{A}} \langle [f] \rangle = \langle \mathcal{A} \rangle = \mathscr{A}$ by construction.

Let $\mathcal{V}$ be an $\mathbb{F}_2$-basis for a complement of $\mathscr{A}$ in $\mathscr{V}$. By definition of $\mathscr{V}$, for each $[f] \in \mathcal{V}$, we can choose $[\gamma_{1,f}], [\gamma_{2,f}] \in [K^\times]$ so that, for $\{i, j\} = \{1, 2\}$, we have $[\gamma_{i,f}]^{1+\sigma_i} = [f]$ and $[\gamma_{i,f}]^{1+\sigma_j} = [1]$. For each $[f] \in \mathcal{V}$, we define $M_{[f]} := \langle [\gamma_{1,f}], [\gamma_{2,f}] \rangle$. We claim that $M_{[f]} \simeq \Omega^1$ and that $M_{[f]}^G = \langle [f] \rangle$. By construction, the appropriate Ω^1-relations are satisfied for $M_{[f]}$, so we need only check that there are not additional relations. For this, observe that any nontrivial relation among $\{[f], [\gamma_{1,f}], [\gamma_{2,f}]\}$ must involve at least one of $[\gamma_{1,f}]$ or $[\gamma_{2,f}]$ since we know that $[f]$ is nontrivial. On the one hand, if we had a nontrivial relation involving $[\gamma_{1,f}]$, then an application of $1 + \sigma_1$ to this relation would tell us that $[f] = [1]$; on the other hand, a nontrivial relation involving $[\gamma_{2,f}]$ would tell us that $[f] = [1]$ after an application of $1 + \sigma_2$. Hence, our set is independent, and so $M_{[f]} \simeq \Omega^1$. This gives $M_{[f]}^G = \langle [f] \rangle$ as well. Let

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

$Y_V = \sum_{[f]\in\mathcal{V}} M_{[f]}$. Indeed, we have $Y_V = \bigoplus_{[f]\in\mathcal{V}} M_{[f]}$ by Lemma 2.1. We also have $Y_V^G = \bigoplus_{[f]\in\mathcal{V}} M_{[f]}^G = \bigoplus_{[f]\in\mathcal{V}} \langle [f] \rangle = \langle \mathcal{V} \rangle$ by construction.

Now, let B be a complement to $\mathscr{V}$ within $\mathscr{B}$, and let C a complement to $\mathscr{V}$ within $\mathscr{C}$. Let B_W and C_W be the subspaces defined in Lemma 3.2. Let $\mathcal{B}_W$ be an $\mathbb{F}_2$-basis for B_W. For each $[b] \in \mathcal{B}_W$, we know that there exist $[\gamma_1], [\gamma_2], [\gamma_3] \in J(K)$ and $\phi_W([b]) = [c] \in C_W$ which solve equation (3.1). Let $M_{[b]} = \langle [b], [c], [\gamma_1], [\gamma_2], [\gamma_3] \rangle$. We claim that $M_{[b]} \simeq \Omega^2$. Certainly, the appropriate Ω^2 relations hold by construction, so we simply need to ensure that there are no additional relations. The elements $[b]$ and $[c]$ are independent since $[b]$ and $[c]$ are each drawn from a complement to $\mathscr{V} = \mathscr{B} \cap \mathscr{C}$ in their respective spaces. Now, if we had a nontrivial $\mathbb{F}_2$-dependence that involved any of $[\gamma_1]$ or $[\gamma_2]$, then an application of $1 + \sigma_1$ would force a nontrivial $\mathbb{F}_2$-dependence on $[b]$ and $[c]$, which we have just seen is not possible. Likewise, a nontrivial $\mathbb{F}_2$-dependence that involves $[\gamma_3]$ would force a nontrivial $\mathbb{F}_2$-dependence between $[b]$ and $[c]$. Hence, the set is independent, and so $M_{[b]} \simeq \Omega^2$. Note this also forces $M_{[b]}^G = \langle [b], [c] \rangle = \langle [b], \phi_W([b]) \rangle$. Let $Y_W = \sum_{[b]\in\mathcal{B}_W} M_{[b]}$. As before, we in fact have $Y_W = \bigoplus_{[b]\in\mathcal{B}_W} M_{[b]}$, and furthermore

$$Y_W^G = \bigoplus_{[b]\in\mathcal{B}_W} M_{[b]}^G = \bigoplus_{[b]\in\mathcal{B}_W} \langle [b], \phi_W([b]) \rangle = B_W \oplus \phi_W(B_W) = B_W \oplus C_W,$$

by Lemma 3.2.

Let $\mathcal{B}_0$ be a basis for a complement to B_W within B. Since $B \subseteq \mathscr{B}$, each $[f] \in \mathcal{B}_0$ has some $[\gamma_f] \in [K^\times]$ so that $[\gamma_f]^{1+\sigma_1} = [f]$ and $[\gamma_f]^{1+\sigma_2} = [1]$. Since $[f] \neq [1]$, we get $M_{[f]} := \langle [\gamma_f] \rangle$ is isomorphic to $\mathbb{F}_2[\overline{G_1}]$, and $M_{[f]}^G = \langle [f] \rangle$. Let $Y_B = \sum_{[f]\in\mathcal{B}_0} M_{[f]}$. Lemma 2.1 again gives $Y_B = \bigoplus_{[f]\in\mathcal{B}_0} M_{[f]}$, and furthermore we have $Y_B^G = \bigoplus_{[f]\in\mathcal{B}_0} M_{[f]}^G = \bigoplus_{[f]\in\mathcal{B}_0} \langle [f] \rangle = \langle \mathcal{B}_0 \rangle$.

Let $\mathcal{C}_0$ be a basis for a complement to C_W within C. Since $C \subseteq \mathscr{C}$, for each $[f] \in \mathcal{C}_0$, there exists some $[\gamma_f] \in [K^\times]$ so that $[\gamma_f]^{1+\sigma_2} = [f]$ and $[\gamma_f]^{1+\sigma_1} = [1]$. Since $[f] \neq [1]$, we get $M_{[f]} := \langle [\gamma_f] \rangle$ is isomorphic to $\mathbb{F}_2[\overline{G_2}]$, and $M_{[f]}^G = \langle [f] \rangle$. Let $Y_C = \sum_{[f]\in\mathcal{C}_0} M_{[f]}$. Once again, we have $Y_C = \bigoplus_{[f]\in\mathcal{C}_0} M_{[f]}$ by Lemma 2.1, and $Y_C^G = \bigoplus_{[f]\in\mathcal{C}_0} M_{[f]}^G = \bigoplus_{[f]\in\mathcal{C}_0} \langle [f] \rangle = \langle \mathcal{C}_0 \rangle$.

Let $\mathcal{D}_0$ be a basis for a complement to $(\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$ within $\mathscr{D}$. By the definition of $\mathscr{D}$, for each $[f] \in \mathcal{D}_0$, there exists some $[\gamma_f] \in [K^\times]$ so that $[\gamma_f]^{1+\sigma_2} = [\gamma_f]^{1+\sigma_1} = [f]$. Since $[f] \neq [1]$, we get $M_{[f]} := \langle [\gamma_f] \rangle$ is isomorphic to $\mathbb{F}_2[\overline{G_3}]$, and $M_{[f]}^G = \langle [f] \rangle$. Let $Y_D = \sum_{[f]\in\mathcal{D}_0} M_{[f]}$. Again, we get $Y_D = \bigoplus_{[f]\in\mathcal{D}_0} M_{[f]}$, and $Y_D^G = \bigoplus_{[f]\in\mathcal{D}_0} M_{[f]}^G = \bigoplus_{[f]\in\mathcal{D}_0} \langle [f] \rangle = \langle \mathcal{D}_0 \rangle$.

Finally, define $\mathcal{F}_0$ to be a basis for a complement to $\mathscr{B} + \mathscr{C} + \mathscr{D}$ within $[F^\times]$. For each $[f] \in \mathcal{F}_0$, we define $M_{[f]} = \langle [f] \rangle$, which is clearly isomorphic to $\mathbb{F}_2$. We let $Y_F = \bigoplus_{[f]\in\mathcal{F}_0} M_{[f]}$.

We have already detailed the fixed parts of each submodule, and we will use this to show that the sum is direct. First, recall that $Y_A^G = \mathscr{A}$ and $Y_V^G = \langle \mathcal{V} \rangle$, where $\mathcal{V}$ is chosen to be a complement to $\mathscr{A}$ in $\mathscr{V}$. Then Lemma 2.1 gives $Y_A + Y_V = Y_A \oplus Y_V$, and additionally we have $(Y_A \oplus Y_V)^G = \mathscr{V}$.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

Next, since $Y_W^G = B_W \oplus C_W$—where B_W and C_W are complements to $\mathscr{V}$ in their respective spaces—Lemma 2.1 gives $(Y_A \oplus Y_V) + Y_W = Y_A \oplus Y_V \oplus Y_W$, and indeed $(Y_A \oplus Y_V \oplus Y_W)^G = \mathscr{V} \oplus B_W \oplus C_W$.

Next, we know that $\mathscr{B} = \mathscr{V} \oplus B_W \oplus \langle \mathcal{B}_0 \rangle$, and since $Y_B^G = \langle \mathcal{B}_0 \rangle$, this means that $Y_A \oplus Y_V \oplus Y_W + Y_B = Y_A \oplus Y_V \oplus Y_W \oplus Y_B$, and $(Y_A \oplus Y_V \oplus Y_W \oplus Y_B)^G = \mathscr{B} \oplus C_W$. Using the facts that $\mathscr{B} \cap \mathscr{C} = \mathscr{V}$, that $Y_C^G = \langle \mathcal{C}_0 \rangle$, and that $\mathscr{C} = \mathscr{V} \oplus C_W \oplus \langle \mathcal{C}_0 \rangle$, Lemma 2.1 gives $Y_A \oplus Y_V \oplus Y_W \oplus Y_B + Y_C = Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C$, and $(Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C)^G = \mathscr{B} + \mathscr{C}$.

For the next term, since $Y_D^G = \langle \mathcal{D}_0 \rangle$, where $\mathcal{D}_0$ is a complement to $(\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$, Lemma 2.1 gives us $Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C + Y_D = Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C \oplus Y_D$, and indeed $(Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C \oplus Y_D)^G = \mathscr{B} + \mathscr{C} + \mathscr{D}$.

Finally, since $Y_F^G = \langle \mathcal{F}_0 \rangle$, where $\mathcal{F}_0$ is a complement to $\mathscr{B} + \mathscr{C} + \mathscr{D}$ in $[F^\times]$, one final application of Lemma 2.1 gives $\widehat{J}^G = [F^\times]$ and

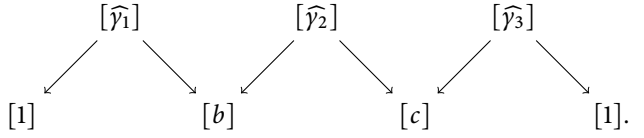
$$\widehat{J} = Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C \oplus Y_D \oplus Y_F. \qquad \blacksquare$$

Corollary 3.4 *Suppose that $[f] \in \mathscr{M}$ for $\mathscr{M} \in \{\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{D}\}$. Then the diagram corresponding to $\mathscr{M}$ has a solution for $[f]$ in which each term of the solution comes from $\widehat{J}$.*

Proof Suppose first that $[f] \in \mathscr{A}$. Since $\mathcal{A}$ is a basis for $\mathscr{A}$, we have $[f] = \prod_{i=1}^n [f_i]$ for appropriately chosen $[f_i] \in \mathcal{A}$. By construction, there exist $[k_i] \in J(K)$ so that $[N_{K/F}(k_i)] = [f_i]$, and so we get $k = \prod_{i=1}^n [k_i]$ has $[N_{K/F}(k)] = [f]$. Hence, the diagram corresponding to $\mathscr{A}$ is solvable for $[f]$ with terms drawn from $\widehat{J}$.

Now, suppose that $[f] \in \mathscr{B}$. Since we know $\mathscr{B} = \mathscr{V} \oplus B_W \oplus \langle \mathcal{B}_0 \rangle$, we can write $[f] = \prod_{i=1}^n [f_i] \prod_{j=1}^m [\widehat{f_j}] \prod_{k=1}^\ell [\widetilde{f_k}]$, where $f_i \in \mathcal{A} \cup \mathcal{V}$, $\widehat{f_j} \in \mathcal{B}_W$, and $\widetilde{f_k} \in \mathcal{B}_0$ are appropriately chosen. Based on the construction of the terms from Y_A, Y_V, Y_W, and Y_B, we have elements $[\gamma_i], [\widehat{\gamma_j}], [\widetilde{\gamma_k}] \in \widehat{J}$ that solve the diagram corresponding to $\mathscr{B}$. Hence, if we let $[\gamma] = \prod_{i=1}^n [\gamma_i] \prod_{j=1}^m [\widehat{\gamma_j}] \prod_{k=1}^\ell [\widetilde{\gamma_k}]$, then the diagram corresponding to $\mathscr{B}$ is solved with $[\gamma]$ and $[f]$. An analogous argument settles the case where $[f] \in \mathscr{C}$.

We have left to settle the statement for $\mathscr{M} = \mathscr{D}$. This will take a bit more work. Since $\mathcal{D}_0$ is a basis for a complement to $(\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$ within $\mathscr{D}$, we can write $[f] = [\hat{f}] \prod_{i=1}^n [f_i]$, where $[\hat{f}] \in (\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$, and with $[f_i] \in \mathcal{D}_0$ appropriately chosen. By construction of Y_D, for each i, we have an element $[\gamma_i]$ so that the diagram for $\mathscr{D}$ is solved with $[\gamma_i]$ and $[f_i]$. Furthermore, since $[\hat{f}] \in (\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$, Lemma 3.1 tells us that $[\hat{f}] = [b][c]$ has the property that equation (3.1) is solvable for $[b]$ and $[c]$:

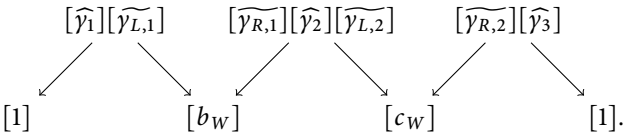


Since B is a complement to $\mathscr{V}$ in $\mathscr{B}$ and C is a complement to $\mathscr{V}$ in $\mathscr{C}$, we can write $[b] = [\nu_1][b_W]$ and $[c] = [\nu_2][c_W]$ for $[\nu_1], [\nu_2] \in \mathscr{V}$ and $[b_W] \in B$ and $[c_W] \in C$. For $i \in \{1, 2\}$, the construction of Y_A and Y_V give $[\widetilde{\gamma_{L,i}}], [\widetilde{\gamma_{R,i}}] \in \widehat{J}$ that accompany $[\nu_i]$ in solving the diagram for $\mathscr{V}$. Note in particular this means that the diagram

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

corresponding to $\mathscr{D}$ is solved for $[\widetilde{\gamma_{L,i}}][\widetilde{\gamma_{R,i}}]$ and $[\nu_i]$. We have left to deal with the $[b_W]$ and $[c_W]$ terms.

From our previous equations, we get



This means that $[b_W] \in B_W$, and, by Lemma 3.2, we have $\phi_W([b_W]) = c_W \in C_W$. Hence, $[b_W] = \prod_{j=1}^m [b_j]$ for $[b_j]$ appropriately chosen from $\mathcal{B}_W$. By the construction of Y_W, we have elements $[\gamma_{1,j}], [\gamma_{2,j}], [\gamma_{3,j}] \in \widehat{J}$ which solve equation (3.1) for $[b_j]$ and $\phi_W([b_j])$. Hence, $\prod_{j=1}^m [\gamma_{1,j}]$, $\prod_{j=1}^m [\gamma_{2,j}]$, and $\prod_{j=1}^m [\gamma_{3,j}]$ solve equation (3.1) for $[b_W]$ and $\prod_{j=1}^m \phi_W([b_j]) = \phi_W(\prod_{j=1}^m [b_j]) = [c_W]$. In particular, the equation corresponding to $\mathscr{D}$ is solved by $\prod_{j=1}^m [\gamma_{1,j}][\gamma_{2,j}][\gamma_{3,j}]$ and $[b_W][c_W]$.

In all, our original element $[f] \in \mathscr{D}$ has now been expressed as $[f] = [\hat{f}] \prod_{i=1}^n [f_i] = [b][c] \prod_{i=1}^n [f_i] = [\nu_1][b_W][\nu_2][c_W] \prod_{i=1}^n [f_i]$, where each of $[\nu_1], [\nu_2], [b_W][c_W]$, and $\prod_{i=1}^n [f_i]$ have some corresponding element $[\gamma] \in \widehat{J}$ which solves the diagram corresponding to $\mathscr{D}$. ∎

4 A module whose fixed part complements $[F^\times]$ in $J(K)^G$

Lemma 2.1 tells us that independent summands of $J(K)$ have independent fixed parts. Since we have already constructed a module whose fixed part is $[F^\times]$, we now are interested in finding a complementary module whose fixed part spans a complement to $[F^\times]$ in $J(K)^G$—at least to the degree that such a goal is achievable at all. Ultimately, this search will culminate in Theorem 4.8 at the end of this section, but to work toward this result, we must first determine precisely which elements from $J(K)^G$ come from $[F^\times]$.

Kummer theory tells us that we can determine whether an element $[\gamma] \in J(K)^G$ comes from $[F^\times]$ by examining the Galois group of the extension it generates over F:

$$[\gamma] \in [F^\times] \backslash \{[1]\} \Leftrightarrow \mathrm{Gal}(K(\sqrt{\gamma})/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

The following result gives a slightly more nuanced view of this phenomenon. Note that in this result—and hence for much of the duration of this section—we use the notation $[\gamma]_i$ to indicate the class of an element $\gamma \in K_i^\times \cap K^{\times 2}$ considered in the set $(K_i^\times \cap K^{\times 2})/K_i^{\times 2}$ for $i \in \{1, 2, 3\}$.

Lemma 4.1 *Suppose that $[\gamma] \in J(K)^G \backslash \{[1]\}$. Then $K(\sqrt{\gamma})/F$ is Galois, and if $\widehat{\sigma_1}$ and $\widehat{\sigma_2}$ represent lifts of $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ to the group $\mathrm{Gal}(K(\sqrt{\gamma})/F)$, then we have*

$$[N_{K/K_1}(\gamma)]_1 = [1]_1 \Leftrightarrow \hat{\sigma}_2^2 = id,$$
$$[N_{K/K_2}(\gamma)]_2 = [1]_2 \Leftrightarrow \hat{\sigma}_1^2 = id,$$
$$[N_{K/K_3}(\gamma)]_3 = [1]_3 \Leftrightarrow (\hat{\sigma}_1\hat{\sigma}_2)^2 = id.$$

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

Proof We consider the first statement first. Observe that we already know that $\hat{\sigma}_2^2$ acts trivially on $\sqrt{a_1}$ and $\sqrt{a_2}$, so we only need to determine the action of $\hat{\sigma}_2^2$ on $\sqrt{\gamma}$. For this, note that

$$\sqrt{\gamma}^{\hat{\sigma}_2^2-1} = \left(\sqrt{\gamma}^{\hat{\sigma}_2+1}\right)^{\hat{\sigma}_2-1} = \left(\pm\sqrt{\gamma^{\sigma_2+1}}\right)^{\hat{\sigma}_2-1}.$$

Since $[\gamma] \in J(K)^G$, we have that $[\gamma]^{\sigma_2+1} = [N_{K/K_1}(\gamma)] = [1]$. Hence, we have $N_{K/K_1}(\gamma) \in K_1^\times \cap K^{\times 2}$, and, by Kummer theory, this means that $N_{K/K_1}(\gamma) = a_2^\varepsilon k_1^2$ for some $\varepsilon \in \{0,1\}$ and $k_1 \in K_1^\times$. Note that $\varepsilon = 0$ if and only if $N_{K/K_1}(\gamma) \in K_1^{\times 2}$, which is equivalent to $[N_{K/K_1}(\gamma)]_1 = [1]_1$. Hence, our previous calculation continues

$$\sqrt{\gamma}^{\hat{\sigma}_2^2-1} = \left(\pm\sqrt{a_2}^{\varepsilon} k_1\right)^{\hat{\sigma}_2-1} = \left(\pm\sqrt{a_2}^{\varepsilon} k_1\right)^{\sigma_2-1} = (-1)^\varepsilon.$$

This gives the desired result.

Similar calculations give the other two results. ∎

Corollary 4.2 *Define* $T : J(K)^G \to \bigoplus_{i=1}^3 (K_i^\times \cap K^{\times 2})/K_i^{\times 2}$ *by*

$$T([\gamma]) = ([N_{K/K_1}(\gamma)]_1, [N_{K/K_2}(\gamma)]_2, [N_{K/K_3}(\gamma)]_3).$$

Then $\ker(T) = [F^\times]$.

Remark 4.3 Note that Kummer theory tells us that each $(K_i^\times \cap K^{\times 2})/K_i^{\times 2}$ consists of only two distinct classes, with representatives drawn from $\{1, a_1, a_2, a_1a_2\}$. For example, $(K_3^\times \cap K^{\times 2})/K_3^{\times 2}$ has $[1]_3 = [a_1a_2]_3$ and $[a_1]_3 = [a_2]_3$ as its elements. For the sake of lightening what would otherwise be fairly weighty notation, when considering elements in the image of T, we will suppress the bracket notation in its coordinates; that is to say, if $T([\gamma]) = ([u]_1, [v]_2, [w]_3)$, then we will instead write $T([\gamma]) = (u, v, w)$.

Our goal, then, is to build a module whose fixed part spans the image of T, ideally while avoiding $[F^\times]$ as much as possible. The first question we consider when looking for such a module is to determine when elements with a nontrivial image under T are themselves in the image of either $1 + \sigma_1$ or $1 + \sigma_2$. We start with the following result.

Lemma 4.4 *If* $\gamma \in K^\times$ *has* $[N_{K/F}(\gamma)] = [1]$, *then* $[N_{K/K_1}(\gamma)], [N_{K/K_2}(\gamma)] \in J(K)^G$, *and*

- $[N_{K/F}(\gamma)]_F = [1]_F \Leftrightarrow T([N_{K/K_1}(\gamma)]) = (1,1,1) \Leftrightarrow T([N_{K/K_2}(\gamma)]) = (1,1,1)$;
- $[N_{K/F}(\gamma)]_F = [a_1]_F \Leftrightarrow T([N_{K/K_1}(\gamma)]) = (1, a_1, a_1) \Leftrightarrow T([N_{K/K_2}(\gamma)]) = (1,1,a_1)$;
- $[N_{K/F}(\gamma)]_F = [a_2]_F \Leftrightarrow T([N_{K/K_1}(\gamma)]) = (1,1,a_1) \Leftrightarrow T([N_{K/K_2}(\gamma)]) = (a_2,1,a_1)$; *and*
- $[N_{K/F}(\gamma)]_F = [a_1a_2]_F \Leftrightarrow T([N_{K/K_1}(\gamma)]) = (1, a_1, 1) \Leftrightarrow T([N_{K/K_2}(\gamma)]) = (a_2,1,1)$.

Proof Observe first that since $[N_{K/F}(\gamma)] = [1]$, Kummer theory tells us that $[N_{K/F}(\gamma)]_F \in \{[1]_F, [a_1]_F, [a_2]_F, [a_1a_2]_F\}$. So let us write $N_{K/F}(\gamma) = f^2 a_1^{\varepsilon_1} a_2^{\varepsilon_2}$. The result then follows from the following calculations:

$$[N_{K/K_1}(N_{K/K_1}(\gamma))]_1 = [N_{K/K_1}(\gamma)^2]_1 = [1]_1,$$
$$[N_{K/K_2}(N_{K/K_1}(\gamma))]_2 = [N_{K/F}(\gamma)]_2 = [f^2 a_1^{\varepsilon_1} a_2^{\varepsilon_2}]_2 = [a_1]_2^{\varepsilon_1},$$

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

$$[N_{K/K_3}(N_{K/K_1}(\gamma))]_3 = [N_{K/F}(\gamma)]_3 = [f^2 a_1^{\varepsilon_1} a_2^{\varepsilon_2}]_3 = [a_1]_3^{\varepsilon_1+\varepsilon_2},$$
$$[N_{K/K_1}(N_{K/K_2}(\gamma))]_1 = [N_{K/F}(\gamma)]_1 = [f^2 a_1^{\varepsilon_1} a_2^{\varepsilon_2}]_1 = [a_2]_1^{\varepsilon_2},$$
$$[N_{K/K_2}(N_{K/K_2}(\gamma))]_2 = [N_{K/K_2}(\gamma)^2]_2 = [1]_2,$$
$$[N_{K/K_3}(N_{K/K_2}(\gamma))]_3 = [N_{K/F}(\gamma)]_3 = [f^2 a_1^{\varepsilon_1} a_2^{\varepsilon_2}]_3 = [a_1]_3^{\varepsilon_1+\varepsilon_2}.$$ ∎

Corollary 4.5 *Suppose that $[\gamma] \in J(K)$ generates a module isomorphic to $\mathbb{F}_2[\overline{G_i}]$ for some $i \in \{1,2,3\}$. Then $T(\langle [\gamma] \rangle^G) = \{(1,1,1)\}$.*

Proof We proceed by cases. If $\langle [\gamma] \rangle \simeq \mathbb{F}_2[\overline{G_1}]$, then we have $[\gamma]^{1+\sigma_2} = [1]$, so that $[N_{K/F}(\gamma)] = [1]$. Since $\langle [\gamma] \rangle^G = \langle [\gamma]^{1+\sigma_1} \rangle$, in this case, our objective is to show that $T([\gamma]^{1+\sigma_1}) = (1,1,1)$. But since $[\gamma]^{1+\sigma_1} = [N_{K/K_2}(\gamma)]$, the previous lemma tells us that if we have $T([\gamma]^{1+\sigma_1}) \neq (1,1,1)$, then we have $(1,1,1) \neq T([N_{K/K_1}(\gamma)]) = T([\gamma]^{1+\sigma_2}) = T([1])$ as well, a contradiction. The same argument gives the result for $i = 2$.

For $i = 3$, a variation on this argument works: we know we have $[N_{K/K_1}(\gamma)] = [N_{K/K_2}(\gamma)]$, and yet the lemma above provides no nontrivial case in which $T([N_{K/K_1}(\gamma)]) = T([N_{K/K_2}(\gamma)])$. ∎

Lemma 4.4 tells us a relationship between the possible values under T for elements from $J(K)^G$ which are in the image of a common element; if two elements $[x]$ and $[y]$ have "compatible" images under T (i.e., allowable in light of Lemma 4.4), is it the case that there exists some $[\gamma]$ so that $[x] = [N_{K/K_1}(\gamma)]$ and $[y] = [N_{K/K_2}(\gamma)]$? The answer to this is generally "no," but there is a weaker version which we will take advantage of.

Lemma 4.6 *Suppose that $[x], [y] \in J(K)^G$ are given, and that $(T([x]), T([y]))$ is either $((1,a_1,a_1),(1,1,a_1))$ or $((1,1,a_1),(a_2,1,a_1))$ or $((1,a_1,1),(a_1,1,1))$. Then there exists some $[\gamma]$ with $[N_{K/F}(\gamma)] = [1]$ so that $T([N_{K/K_1}(\gamma)]) = T([x])$ and $T([N_{K/K_2}(\gamma)]) = T([y])$.*

Proof Our approach will be to argue that the appearance of these elements in the image of T guarantees the solvability of certain embedding problems, from which we deduce the solvability of certain equations involving norms.

We first handle the case where $\mathrm{im}(T)$ contains $\{(1,a_1,a_1),(1,1,a_1)\}$. Since $T([x]) = (1,a_1,a_1)$, we know from Lemma 4.1 that in $K(\sqrt{x})/F$ the generators $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ extend to elements $\hat{\sigma}_1, \hat{\sigma}_2 \in \mathrm{Gal}(K(\sqrt{x})/F)$ which satisfy the relations

$$\hat{\sigma}_2^2 = \hat{\sigma}_1^4 = (\hat{\sigma}_1\hat{\sigma}_2)^4 = \mathrm{id}.$$

Hence, $\mathrm{Gal}(K(\sqrt{x})/F) \twoheadrightarrow \mathrm{Gal}(K/F)$ solves the embedding problem $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and in particular K_1/F embeds in a cyclic extension of degree 4. By [2, Theorem 3], we have $-1 \in N_{K_1/F}(K_1^\times)$; since we have $-a_1 = (\sqrt{a_1})^{1+\sigma_1} = N_{K_1/F}(\sqrt{a_1})$, it therefore follows that $a_1 \in N_{K_1/F}(K_1^\times)$, say $a_1 = N_{K_1/F}(k_1)$ for $k_1 \in K_1^\times$.

On the other hand, since $T([y]) = (1,1,a_1)$, we know from Lemma 4.1 that the generators $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ extend to elements $\tilde{\sigma}_1, \tilde{\sigma}_2 \in \mathrm{Gal}(K(\sqrt{y})/F)$ that satisfy

$$\tilde{\sigma}_2^2 = \tilde{\sigma}_1^2 = (\tilde{\sigma}_1\tilde{\sigma}_2)^4 = \mathrm{id}.$$

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

From this, we see that $\mathrm{Gal}(K(\sqrt{y})/F) \twoheadrightarrow \mathrm{Gal}(K/F)$ solves the embedding problem $D_4 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where the kernel of the latter surjection is $\langle(\tilde{\sigma}_1\tilde{\sigma}_2)^2\rangle$. By a well-known result for the solvability of such embedding problems (see, e.g., [16, Proposition III.3.3]), we therefore have $a_1 \in N_{K_2/F}(K_2^\times)$, say $a_1 = N_{K_2/F}(k_2)$ for $k_2 \in K_2^\times$.

By [30, Lemma 2.14], there exists some $\gamma \in K^\times$ and $f \in F^\times$ so that $N_{K/K_1}(\gamma) = fk_1$ and $N_{K/K_2}(\gamma) = fk_2$. In particular, we have $[N_{K/F}(\gamma)]_F = [f^2a_1]_F = [a_1]_F$. An application of Lemma 4.4 finishes this case.

The second case is effectively identical to the first. For the last case, note that the images we are given provide two D_4-extensions over K/F, one in which σ_1 extends to an element of order 4, and another where σ_2 extends to an element of order 4. In the former case, we then get $a_1a_2 \in N_{K_2/F}(K_2^\times)$, and in the latter, we get $a_1a_2 \in N_{K_1/F}(K_1^\times)$. From here, the proof proceeds as before. ∎

Remark 4.7 The use of [30, Lemma 2.14] amounts to an appeal to Hilbert 90 for biquadratic extensions. See [10].

We are now prepared for the main result of this section.

Theorem 4.8 *There exists $X \subseteq J(K)$ with $T(X^G) = \mathrm{im}(T)$, so that*

$$X \simeq \begin{cases} \{[1]\}, & \text{if } \dim(\mathrm{im}(T)) = 0, \\ \mathbb{F}_2, & \text{if } \dim(\mathrm{im}(T)) = 1, \\ \Omega^{-1}, & \text{if } \dim(\mathrm{im}(T)) = 2 \text{ and } \mathrm{im}(T) \text{ is one of the "coordinate planes,"} \\ \mathbb{F}_2 \oplus \mathbb{F}_2, & \text{if } \dim(\mathrm{im}(T)) = 2 \text{ and } \mathrm{im}(T) \text{ is not one of the "coordinate planes,"} \\ \Omega^{-2}, & \text{if } \dim(\mathrm{im}(T)) = 3 \text{ and } T\left([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]\right) \neq \{(1,1,1)\}, \\ \Omega^{-1} \oplus \Omega^{-1}, & \text{if } \dim(\mathrm{im}(T)) = 3 \text{ and } T\left([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]\right) = \{(1,1,1)\}. \end{cases}$$

In all cases except the last, we have $[F^\times] \cap X^G = \{[1]\}$; in the last case, we have $\dim(X^G \cap [F^\times]) = 1$ and $X^G \cap (\mathscr{B} + \mathscr{C} + \mathscr{D}) = \{[1]\}$.

Proof We proceed by cases based on $\dim(\mathrm{im}(T))$. First, if $\dim(\mathrm{im}(T)) = 1$, then let $[x] \in J(K)^G$ be given so that $T([x]) \neq (1,1,1)$. Then $X := \langle[x]\rangle$ has the desired properties.

Now, suppose that $\dim(\mathrm{im}(T)) = 2$. By Lemma 4.6, we know that if $\mathrm{im}(T)$ is any of

$$\langle(1, a_1, a_1), (1,1,a_1)\rangle = \{(1,w,z) : w \in (K_2^\times \cap K^{\times 2})/K_2^{\times 2}, z \in (K_3^\times \cap K^{\times 2})/K_3^{\times 2}\},$$
$$\langle(1,1,a_1), (a_2,1,a_1)\rangle = \{(w,1,z) : w \in (K_1^\times \cap K^{\times 2})/K_1^{\times 2}, z \in (K_3^\times \cap K^{\times 2})/K_3^{\times 2}\}, \text{ or}$$
$$\langle(1, a_1, 1), (a_1,1,1)\rangle = \{(w,z,1) : w \in (K_1^\times \cap K^{\times 2})/K_1^{\times 2}, z \in (K_2^\times \cap K^{\times 2})/K_2^{\times 2}\},$$

then we can find some $[\gamma] \in J(K)$ with $[N_{K/F}(\gamma)] = [1]$ so that $\left\langle T\left([N_{K/K_1}(\gamma)]\right), T\left([N_{K/K_2}(\gamma)]\right)\right\rangle = \mathrm{im}(T)$. It is easy to see that $X := \langle[\gamma]\rangle \simeq \Omega^{-1}$, and since the nontrivial fixed elements in this module have nontrivial images under T, we get $X^G \cap [F^\times] = \{[1]\}$.

On the other hand, if $\dim(\mathrm{im}(T)) = 2$ but $\mathrm{im}(T)$ is none of the three subspaces above, then let $[x_1], [x_2] \in J(K)^G$ be given so that $\{T([x_1]), T([x_2])\}$ forms a basis for $\mathrm{im}(T)$; we then set $X := \langle[x_1], [x_2]\rangle \simeq \mathbb{F}_2 \oplus \mathbb{F}_2$, with $X \cap [F^\times] = \{[1]\}$.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

Now, suppose that $\dim(\mathrm{im}(T)) = 3$. First, consider the case where $T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]) \neq \{(1,1,1)\}$, and let $[x]$ be given so that $[N_{K/K_1}(\gamma_2)] = [x] = [N_{K/K_2}(\gamma_1)]$ for some $[\gamma_1], [\gamma_2] \in J(K)$ and with $T([x]) \neq (1,1,1)$. (Note that since $[x]$ is in the image of N_{K/K_1} and N_{K/K_2}, it is automatically in $J(K)^G$; hence, it makes sense to evaluate its image under T.) Lemma 4.4 tells us that $T([x]) = (1,1,a_1)$, and furthermore that $T([N_{K/K_1}(\gamma_1)]) = (1,a_1,a_1)$ and $T([N_{K/K_2}(\gamma_2)]) = (a_2,1,a_1)$. We claim that $X := \langle [\gamma_1], [\gamma_2] \rangle \simeq \Omega^{-2}$; certainly, the appropriate relations hold, so we only need to check that the module is five-dimensional. Note that $\{[N_{K/K_1}(\gamma_1)], [x], [N_{K/K_2}(\gamma_2)]\}$ must be independent since their images under T are independent, and hence any nontrivial dependence must involve $[\gamma_1]$ or $[\gamma_2]$. However, an application of $1+\sigma_1$ (or $1+\sigma_2$) to such a relation creates a nontrivial relation among $\{[N_{K/K_1}(\gamma_1)], [x], [N_{K/K_2}(\gamma_2)]\}$, contrary to their independence. Since we have $X \simeq \Omega^{-2}$, we get $X^G = \langle [N_{K/K_1}(\gamma_1)], [x], [N_{K/K_2}(\gamma_2)] \rangle$, whence $X^G \cap [F^\times] = \{[1]\}$.

Alternatively, suppose that $\dim(\mathrm{im}(T)) = 3$, but $T([N_{K/K_1}(K^\times) \cap [N_{K/K_2}(K^\times)]) = \{(1,1,1)\}$. Lemma 4.6 gives us elements $[\gamma_1], [\gamma_2] \in J(K)$ so that

$$\begin{aligned} T([N_{K/K_1}(\gamma_1)]) &= (1, a_1, a_1), \\ T([N_{K/K_2}(\gamma_1)]) &= (1,1,a_1) = T([N_{K/K_1}(\gamma_2)]), \\ T([N_{K/K_2}(\gamma_2)]) &= (a_2, 1, a_1). \end{aligned}$$

We define $X = \langle [\gamma_1], [\gamma_2] \rangle$. One sees that $\langle [\gamma_1] \rangle \simeq \langle [\gamma_2] \rangle \simeq \Omega^{-1}$ in the same manner as above (these modules satisfy the appropriate relations by definition, and one can argue they generate a module of the appropriate dimension by leveraging the independence of the image of their fixed components under T). We claim that $X \simeq \Omega^{-1} \oplus \Omega^{-1}$; for the sake of contradiction, then, assume instead that $\langle [\gamma_1] \rangle \cap \langle [\gamma_2] \rangle \neq \{[1]\}$. By Lemma 2.1, this implies that there is some $[x] \neq [1]$ with $[x] \in \langle [\gamma_1] \rangle^G \cap \langle [\gamma_2] \rangle^G$. Considering images under T and using Lemma 4.4, we must have $[N_{K/K_2}(\gamma_1)] = [x] = [N_{K/K_1}(\gamma_2)]$, contrary to the assumption in this case that $T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]) = \{(1,1,1)\}$. Hence, we get $X \simeq \Omega^{-1} \oplus \Omega^{-1}$.

Finally, we check that $\dim(X^G \cap [F^\times]) = 1$ with $X^G \cap (\mathscr{B} + \mathscr{C} + \mathscr{D}) = \{[1]\}$. The former follows from the rank-nullity theorem applied to the function T; in fact, we see that $X^G \cap [F^\times] = \{[1], [N_{K/K_2}(\gamma_1)][N_{K/K_1}(\gamma_2)]\}$. For the latter, suppose instead that $[N_{K/K_2}(\gamma_1)][N_{K/K_1}(\gamma_2)] \in \mathscr{B} + \mathscr{C} + \mathscr{D}$. Then we get $[N_{K/K_2}(\gamma_1)][N_{K/K_1}(\gamma_2)] = [f_{\mathscr{B}}][f_{\mathscr{C}}][f_{\mathscr{D}}]$ for some $[f_{\mathscr{B}}] \in \mathscr{B}$, $[f_{\mathscr{C}}] \in \mathscr{C}$ and $[f_{\mathscr{D}}] \in \mathscr{D}$; in particular, this means we have elements $[\gamma_{\mathscr{B}}], [\gamma_{\mathscr{C}}], [\gamma_{\mathscr{D}}] \in J(K)$ which solve the relevant diagrams from Figure 4. One can then check that

$$\begin{aligned} N_{K/K_1}([\gamma_2][\gamma_{\mathscr{C}}]) &= [N_{K/K_1}(\gamma_2)][f_{\mathscr{C}}] = [N_{K/K_2}(\gamma_1)][f_{\mathscr{B}}][f_{\mathscr{D}}] \\ &= N_{K/K_2}([\gamma_1][\gamma_{\mathscr{B}}][\gamma_{\mathscr{D}}]). \end{aligned}$$

This element is conspicuously an element in $[N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]$, and since $\ker(T) = [F^\times]$, we get that $T([N_{K/K_2}(\gamma_1)][f_{\mathscr{B}}][f_{\mathscr{D}}]) = T([N_{K/K_2}(\gamma_1)]) \neq \{(1,1,1)\}$. This runs contrary to the overriding assumption in this case, that $T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]) = \{(1,1,1)\}$. ∎

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

5 Proof of Theorem 1.1

We need one final preparatory result, which is again a manifestation of Hilbert 90 in the biquadratic case.

Lemma 5.1 *Let* $\{\ell, m, n\} = \{1, 2, 3\}$. *If* $f \in F^\times$ *has* $[f] \in [N_{K/K_\ell}(K^\times)]$, *then* $[f] \in [N_{K_m/F}(K_m^\times)][N_{K_n/F}(K_n^\times)]$.

Proof We prove the result when $\ell = 3$, $m = 1$, and $n = 2$; the other results follow by the symmetry of the fields K_1, K_2, and K_3.

First, we argue that if $f \in F^\times$ has $[f] \in [N_{K/K_3}(K^\times)]$, then

$$\frac{f}{a_1^\varepsilon} = N_{K/K_3}(\tilde{k}) \tag{5.1}$$

for some $\tilde{k} \in K^\times$ and $\varepsilon \in \{0, 1\}$. To see this, note that $f = k^{1+\sigma_1\sigma_1}\hat{k}^2$ for some $k, \hat{k} \in K$. Solving for $\hat{k}^2$ and using the fact that $F \subseteq K_3$, we then have $\hat{k}^2 \in K_3$. However, this means $\hat{k}^2 \in K^{\times 2} \cap K_3^\times$, so by Kummer theory, we get $\hat{k}^2 = k_3^2 a_1^\varepsilon$, where $k_3 \in K_3^\times$ and $\varepsilon \in \{0, 1\}$. Naturally, we have $k_3^2 = N_{K/K_3}(k_3)$, so that our original expression becomes

$$f = k^{1+\sigma_1\sigma_2}\hat{k}^2 = k^{1+\sigma_1\sigma_2}k_3^2 a_1^\varepsilon = N_{K/K_3}(kk_3)a_1^\varepsilon.$$

Setting $\tilde{k} = kk_3$ and dividing through by a_1^ε gives equation (5.1).

Now, we argue that

$$F^\times \cap N_{K/K_3}(K^\times) \subseteq N_{K_1/F}(K_1^\times) \cdot N_{K_2/F}(K_2^\times). \tag{5.2}$$

For this, suppose that we have elements $g \in F^\times$ and $k \in K^\times$ so that $g = N_{K/K_3}(k)$. Now, $k = f_1 + f_2\sqrt{a_1} + f_3\sqrt{a_2} + f_4\sqrt{a_1a_2}$ for some $f_1, f_2, f_3, f_4 \in F^\times$, and so by assumption we get

$$g = N_{K/K_3}(k) = (f_1^2 - a_1f_2^2 - a_2f_3^2 + a_1a_2f_4^2) + \sqrt{a_1a_2}(2f_1f_4 - 2f_2f_3).$$

However, since $g \in F^\times$, we must have $f_1f_4 = f_2f_3$. Our goal is to write g as an element of $N_{K_1/F}(K_1^\times) \cdot N_{K_2/F}(K_2^\times)$, which means we would like to find $h_1, h_2, h_3, h_4 \in F$ so that $h_1 + h_2\sqrt{a_1} \in K_1$ and $h_3 + h_4\sqrt{a_2} \in K_2$ yield

$$g = N_{K_1/F}(h_1 + h_2\sqrt{a_1}) \cdot N_{K_2/F}(h_3 + h_4\sqrt{a_2}) = (h_1^2 - h_2^2a_1)(h_3^2 - h_4^2a_2).$$

In other words, we need to solve

$$f_1^2 - a_1f_2^2 - a_2f_3^2 + a_1a_2f_4^2 = (h_1^2 - h_2^2a_1)(h_3^2 - h_4^2a_2).$$

We proceed by cases. First, suppose that $f_1 = 0$. Hence, we must have either $f_2 = 0$ or $f_3 = 0$. Note if $f_2 = 0$, then our expression for g becomes

$$g = -a_2f_3^2 + a_1a_2f_4^2 = (f_3^2 - f_4^2a_1)(0^2 - 1^2a_2).$$

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

A similar computation settles the case where $f_3 = 0$. So now suppose that $f_1 \neq 0$, and observe that since $f_4 = \frac{f_2 f_3}{f_1}$, we have

$$f_1^2 - f_2^2 a_1 - f_3^2 a_2 + f_4^2 a_1 a_2 = \left(f_1^2 - f_2^2 a_1\right)\left(1^2 - \frac{f_3^2}{f_1^2} a_2\right).$$

With both (5.1) and (5.2) in hand, we can prove the lemma. If we apply (5.2) to $\frac{f}{a_1^\varepsilon}$ from (5.1), then we see that

$$\frac{f}{a_1^\varepsilon} \in N_{K_1/F}(K_1^\times) \cdot N_{K_2/F}(K_2^\times).$$

However, since $[a_1] = [1]$, we get the desired result. ∎

We are now ready for the proof of the main result of this paper. Our basic strategy is to show that the modules $\widehat{J}$ and X from Theorems 3.3 and 4.8 provide the desired decomposition, although in the case where $\dim(\mathrm{im}(T)) = 3$ and $T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]) = \{(1,1,1)\}$ we will need to make a small adjustment to $\widehat{J}$—removing a single trivial summand—to achieve our result.

Proof Let $\widehat{J}$ be the module from Theorem 3.3, and let X be the module from Theorem 4.8.

If we are not in the case where $\dim(\mathrm{im}(T)) = 3$ and $T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)]) = \{(1,1,1)\}$, then define $\widetilde{J} = \widehat{J}$. Otherwise, note that, in the final case of Theorem 4.8, we have a unique $[x_0] \in X^G \cap [F^\times]$, and that $[x_0] \notin \mathscr{B} + \mathscr{C} + \mathscr{D}$. Now, in the construction of $\widehat{J}$, the summand Y_F is chosen as the span of $\mathcal{F}_0$, where $\mathcal{F}_0$ is an arbitrary basis for a complement of $\mathscr{B} + \mathscr{C} + \mathscr{D}$ within $[F^\times]$ (see the definition of $\mathcal{F}_0$ in Theorem 3.3). Since $[x_0] \in [F^\times] \backslash (\mathscr{B} + \mathscr{C} + \mathscr{D})$, we can assume that $[x_0] \in \mathcal{F}_0$. In this case, we define $\tilde{Y}_F = \sum_{[f] \in \mathcal{F}_0 \backslash \{[x_0]\}} \langle [f] \rangle = \bigoplus_{[f] \in \mathcal{F}_0 \backslash \{[x_0]\}} \langle [f] \rangle$, and set

$$\widetilde{J} = Y_A + Y_V + Y_W + Y_B + Y_C + Y_D + \tilde{Y}_F = Y_A \oplus Y_V \oplus Y_W \oplus Y_B \oplus Y_C \oplus Y_D \oplus \tilde{Y}_F.$$

(That is, the module $\widetilde{J}$ is just the result of removing the summand $\langle [x_0] \rangle$ from $\widehat{J}$.)

In either case, we will show that $J(K) = \widetilde{J} \oplus X$. Of course, we have $\widetilde{J} + X \subseteq J(K)$; furthermore, our construction of $\widetilde{J}$ gives $X^G \cap \widetilde{J} = \{[1]\}$, so that $\widetilde{J} + X = \widetilde{J} \oplus X$. Hence, we only need to verify that $J(K) \subseteq \widetilde{J} + X$. We do this by examining the possible isomorphism classes for $\langle [\gamma] \rangle$, where $[\gamma] \in J(K)$.

First, suppose that $\langle [\gamma] \rangle \simeq \mathbb{F}_2$, so that $[\gamma] \in J(K)^G$. If $[\gamma] \in [F^\times]$, then since $[F^\times] = \widehat{J}^G \subseteq \widetilde{J}^G \oplus X^G$, we have $[\gamma] \in \widetilde{J} + X$. Otherwise, we have $T([\gamma]) \neq (1,1,1)$, in which case by Theorem 4.8 there exists some $[x] \in X^G$ with $T([\gamma]) = T([x])$. We then have $[\gamma][x] \in [F^\times]$, and from the previous case, this gives $[\gamma][x] \in \widetilde{J} + X$. Since $[x] \in \widetilde{J} + X$, we get $[\gamma] \in \widetilde{J} + X$.

Now, suppose that $\langle [\gamma] \rangle \simeq \mathbb{F}_2[\overline{G_1}]$. Corollary 4.5 tells us that $[\gamma]^{1+\sigma_1} \in [F^\times]$, and so $[\gamma]^{1+\sigma_1} \in \mathscr{B}$. Corollary 3.4 tells us that there exists some $[\tilde{\gamma}] \in \widehat{J}$ so that $[\tilde{\gamma}]^{1+\sigma_2} = [1]$ and $[\tilde{\gamma}]^{1+\sigma_1} = [\gamma]^{1+\sigma_1}$; in fact, since $\widehat{J}$ and $\widetilde{J}$ differ by only a trivial summand, we can assume $[\tilde{\gamma}] \in \widetilde{J}$ as well. However, then, we get $[\gamma][\tilde{\gamma}] \in J(K)^G$, so by the previous case we have $[\gamma][\tilde{\gamma}] \in \widetilde{J} + X$. Since $[\tilde{\gamma}] \in \widetilde{J} + X$ already, this gives $[\gamma] \in \widetilde{J} + X$.

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

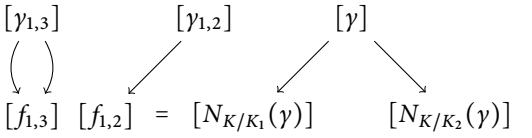


Figure 5: Decomposing $[N_{K/K_1}(\gamma)]$ in terms of solutions to the diagrams for $\mathscr{C}$ and $\mathscr{D}$.

The cases where $\langle[\gamma]\rangle$ is isomorphic to either $\mathbb{F}_2[\overline{G_2}]$ or $\mathbb{F}_2[\overline{G_3}]$ follow the same argument as the case $\mathbb{F}_2[\overline{G_1}]$ above.

Now, suppose that $\langle[\gamma]\rangle \simeq \Omega^{-1}$, and first consider the case where $T(\langle[\gamma]\rangle^G) = \{(1,1,1)\}$. By Corollary 4.2 and Lemma 5.1, we have $[N_{K/K_1}(\gamma)] \in [N_{K/K_1}(K^\times)] \cap [F^\times] = [N_{K_2/F}(K_2^\times)][N_{K_3/F}(K_3^\times)]$, say $[N_{K/K_1}(\gamma)] = [f_{1,2}][f_{1,3}]$, where for $i \in \{2,3\}$ we have $[f_{1,i}] = [N_{K_i/F}(k_i)]$ for some $k_i \in K_i^\times$. This means that $[f_{1,2}] \in \mathscr{C}$ and $[f_{1,3}] \in \mathscr{D}$, so by Corollary 3.4 there exists $[\gamma_{1,i}] \in \widehat{J}$ with $[\gamma_{1,i}]$ and $[f_{1,i}]$ providing a solution to the appropriate diagram; since $\widehat{J}$ and $\widetilde{J}$ differ only by a trivial summand, we can assume that $[\gamma_{1,i}] \in \widetilde{J}$ for $i \in \{2,3\}$. (See Figure 5 for a graphical description of these relationships.)

Consider the element $[\tilde{\gamma}] = [\gamma][\gamma_{1,2}][\gamma_{1,3}]$. One sees that $[\tilde{\gamma}]^{1+\sigma_2} = [1]$, and that $[\tilde{\gamma}]^{1+\sigma_1} = [N_{K/K_2}(\gamma)][f_{1,3}]$. Hence, $\langle[\tilde{\gamma}]\rangle$ is isomorphic to either $\{[1]\}$ or $\mathbb{F}_2$ or $\mathbb{F}_2[\overline{G_1}]$. Our previous cases, therefore, allow us to conclude $[\tilde{\gamma}] \in \widetilde{J} + X$. Since $[\gamma_{1,2}], [\gamma_{1,3}] \in \widetilde{J}$, we have $[\gamma] \in \widetilde{J} + X$.

If $T(\langle[\gamma]\rangle^G) \neq \{(1,1,1)\}$, then Lemma 4.4 gives us that precisely one of the following holds:

- $T([N_{K/K_1}(\gamma)]) = (1, a_1, a_1)$ and $T([N_{K/K_2}(\gamma)]) = (1, 1, a_1)$; or
- $T([N_{K/K_1}(\gamma)]) = (1, 1, a_1)$ and $T([N_{K/K_2}(\gamma)]) = (a_2, 1, a_1)$; or
- $T([N_{K/K_1}(\gamma)]) = (1, a_1, 1)$ and $T([N_{K/K_2}(\gamma)]) = (a_2, 1, 1)$.

In any of these cases, our construction for X (see the second case in Theorem 4.8) gives an element $[x] \in X$ so that $T([N_{K/K_1}(\gamma)]) = T([N_{K/K_1}(x)])$ and $T([N_{K/K_2}(\gamma)]) = T([N_{K/K_2}(x)])$. Hence, the images of $[\gamma][x]$ under $1+\sigma_1$ and $1+\sigma_2$ both lie in $[F^\times]$, and so $\langle[\gamma][x]\rangle$ falls into one of the previous cases. (For example, if $([\gamma][x])^{1+\sigma_1}$ and $([\gamma][x])^{1+\sigma_2}$ are independent, then $\langle[\gamma][x]\rangle \simeq \Omega^{-1}$ and $T(\langle[\gamma][x]\rangle^G) = \{(1,1,1)\}$. This is precisely the previous case.) We therefore get $[\gamma][x] \in \widetilde{J} + X$, whence $[\gamma] \in \widetilde{J} + X$.

The final case to consider is when $\langle[\gamma]\rangle \simeq \mathbb{F}_2[G]$. In this case, note that $[N_{K/F}(\gamma)] \in \mathscr{A}$, and Corollary 3.4 gives us some element $[\tilde{\gamma}] \in \widehat{J}$ (which we may assume is in $\widetilde{J}$ since $\widetilde{J}$ and $\widehat{J}$ differ only by a trivial summand) so that $[N_{K/F}(\tilde{\gamma})] = [N_{K/F}(\gamma)]$. From this, we get that $\langle[\gamma][\tilde{\gamma}]\rangle$ is not free, and so is one of the previous isomorphism types. As usual, this gives us $[\gamma] \in \widetilde{J} + X$. ∎

6 Some realizability results

Theorem 1.1 tells us that there are a limited number of summands that could possibly appear in a decomposition of $J(K)$, but is it the case that each of these summand

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

types occurs for at least one biquadratic extension K/F? In this section, we offer some partial results concerning this kind of realizability question, focusing particularly on the possible structures for the X summand from Theorem 1.1. For a more complete treatment of this problem of realizing the various summands, the reader is encouraged to consult [9], which enhances the current work by exploring its connection to the Brauer group $\mathrm{Br}(F)$.

The X summand takes on one of six possible structures, with the various possibilities determined by the image of the function T from Section 4 (as detailed in Theorem 4.8). To determine whether these structures are realizable, we will view the conditions found in Theorem 4.8 through the lens of Galois embedding problems via Lemma 4.1.

First, we introduce some terminology. Note that since K/F is a biquadratic extension with intermediate fields K_1, K_2, and K_3, if there exists some extension L/K which is Galois over F with $\mathrm{Gal}(L/F) \simeq D_4$, then there is a unique $i \in \{1,2,3\}$ so that $\mathrm{Gal}(L/K_i) \simeq \mathbb{Z}/4\mathbb{Z}$. We will refer to such an extension as a D_4-extension of type i. Likewise, if there is an extension L/K with $\mathrm{Gal}(L/F) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then there is a unique $i \in \{1,2,3\}$ so that there exists some field $\widetilde{L}$ with $K_i \subsetneq \widetilde{L} \subsetneq L$ and $\mathrm{Gal}(\widetilde{L}/F) \simeq \mathbb{Z}/4\mathbb{Z}$. We will refer to such an extension as a $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension of type i.

Lemma 4.1 tells us that if $[\gamma] \in J(K)^G$, then the Galois group of $K(\sqrt{\gamma})/F$ can be computed entirely in terms of $T([\gamma])$. For example, suppose that $T([\gamma]) = (a_2, 1, 1)$. By Lemma 4.1, we see that $K(\sqrt{\gamma})/F$ is a D_4-extension of type 1. Similarly, if $T([\gamma]) = (1, a_1, 1)$ or $T([\gamma]) = (1, 1, a_1)$, then $K(\sqrt{\gamma})/F$ is a D_4-extension of type 2 or 3 (respectively). We also have that $T([\gamma]) \in \{(a_2, a_1, 1), (a_2, 1, a_1), (1, a_1, a_1)\}$ implies that $K(\sqrt{\gamma})/F$ is a $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension (of types 3, 2, and 1, respectively). If $T([\gamma]) = (a_2, a_1, a_1)$, then $K(\sqrt{\gamma})/F$ is a Q_8-extension. Finally, if $T([\gamma]) = (1, 1, 1)$, then $\mathrm{Gal}(K(\sqrt{\gamma})/F)$ is elementary 2-abelian of rank 3. Since each of the possible values of $T([\gamma])$ yields a distinct Galois group, this dictionary works both ways: the structure of the Galois group of a given $K(\sqrt{\gamma})/F$ determines the value of $T([\gamma])$.

Happily, these types of embedding problems have already been studied extensively. For example, in [17], one finds that a quadratic extension $E(\sqrt{a})/E$ embeds in a $\mathbb{Z}_4$-extension if and only if $a = x^2 + y^2$ for $x, y \in E$. Likewise, a biquadratic extension $E(\sqrt{a}, \sqrt{b})/E$ embeds in a D_4-extension L/E for which $\mathrm{Gal}(L/E(\sqrt{b})) \simeq \mathbb{Z}/4\mathbb{Z}$ if and only if $b = ay^2 - x^2$ for some $x, y \in E$. Finally, a biquadratic extension $E(\sqrt{a}, \sqrt{b})/E$ embeds in a Q_8-extension if and only if there are $e_1, e_2, e_3, f_1, f_2, f_3 \in E$ with $a = \sum_{i=1}^3 e_i^2$ and $b = \sum_{i=1}^3 f_i^2$ and $\sum_{i=1}^3 e_i f_i = 0$. Hence, we can determine if a given biquadratic extension K/F has elements $[\gamma] \in J(K)^G$ with prescribed values under T by determining whether certain equations hold over F.

Example 6.1 Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{7}, \sqrt{-5})$. (Following our previous conventions, this means $a_1 = 7$ and $a_2 = -5$.) None of the elements from $\{7, -5, -35\}$ be written as a sum of two rational squares, and hence K/F does not embed in any type of $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension. Hence, no element from $\{(a_2, a_1, 1), (a_2, 1, a_1), (1, a_1, a_1)\}$ is in $\mathrm{im}(T)$. We can also clearly see that $7 = -5y^2 - x^2$ has no rational solutions, so K/F does not embed in a D_4-extension of type 1; therefore, $(a_2, 1, 1) \notin \mathrm{im}(T)$. Likewise $-5 = -35y^2 - x^2$ and $-35 = -5y^2 - x^2$ have no rational solutions. For example, a rational solution to $-5 = -35y^2 - x^2$ would imply an integral solution to $u^2 = 7v^2 + 5w^2$ for

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

which $5 \nmid u$ and $5 \nmid v$. One sees this is impossible by examining this equation modulo 5. Because these equations have no rational solutions, it follows that K/F does not embed in a D_4-extension of type 2 or 3 either. Hence, $\{(1, a_1, 1), (1, 1, a_1)\} \notin \mathrm{im}(T)$. Finally, since -5 is conspicuously not a sum of three rational squares, we have that K/F does not embed in a Q_8-extension, and so $(a_2, a_1, a_1) \notin \mathrm{im}(T)$. Hence, $\mathrm{im}(T) = \{(1,1,1)\}$, and by Theorem 4.8, we have $X = \{[1]\}$.

Example 6.2 Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{7}, \sqrt{-1})$. We see that K/F does not embed in any $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension since none of 7, -1, nor -7 is a sum of two rational squares; it does not embed in a D_4-extension of type 1 or 3 since $7 = -y^2 - x^2$ and $-7 = -y^2 - x^2$ have no rational solutions; and it does not embed in a Q_8-extension since -1 is not a sum of three rational squares. It does, however, embed in a D_4-extension of type 2 since $-1 = -7y^2 - x^2$ has a rational solution. Hence, $\mathrm{im}(T) = \{(1,1,1), (1, a_1, 1)\}$, and so $X \simeq \mathbb{F}_2$.

Example 6.3 Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$. Since 2 is a sum of two rational squares but -1 and -2 are not, we see that K/F embeds in a $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extension of type 1, but not of type 2 or 3. It is also the case that $2 = -y^2 - x^2$ has no rational solutions, but $-1 = 2y^2 - x^2$ and $-2 = 2y^2 - x^2$ do have rational solutions, and hence K/F embeds in D_4-extensions of types 2 and 3, but not type 1. We also have that -1 is not a sum of three rational squares, so K/F does not embed in a Q_8-extension. Taken together, this means that $\mathrm{im}(T) = \{(1,1,1), (1, a_1, a_1), (1, a_1, 1), (1, 1, a_1)\}$, which is one of the coordinate planes (the "yz-plane"). Hence, from Theorem 4.8, we have $X \simeq \Omega^{-1}$.

Example 6.4 Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$. We know that each of 5, 13, and 65 can be written as a sum of two rational (indeed, integral) squares, and hence K/F embeds in $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$-extensions of types 1–3. Therefore, $\{(1,1,1), (a_2, a_1, 1), (a_2, 1, a_1), (1, a_1, a_1)\} \subseteq \mathrm{im}(T)$. On the other hand, there is no rational solution to $5 = 13y^2 - x^2$, since such a solution would imply an integral solution to $5u^2 = 13v^2 - w^2$. (After ensuring that 5 does not divide all of u, v, and w, one examines the equation modulo 5.) Hence, K/F does not embed in a D_4-extension of type 1, and so $(a_2, 1, 1) \notin \mathrm{im}(T)$. Since T is an $\mathbb{F}_2$-space, we get $\{(1,1,1), (a_2, a_1, 1), (a_2, 1, a_1), (1, a_1, a_1)\} = \mathrm{im}(T)$. By Theorem 4.8, we have $X \simeq \mathbb{F}_2 \oplus \mathbb{F}_2$.

Example 6.5 Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{5}, \sqrt{41})$. Since 5, 41, and 205 are all expressible as sums of two rational squares, and since we can write $5 = (2)^2 + (1)^2 + 0^2$ and $41 = (-1)^2 + (2)^2 + (6)^2$, we see that $\{(a_2, a_1, 1), (a_2, 1, a_1), (1, a_1, a_1), (a_2, a_1, a_1)\} \subseteq \mathrm{im}(T)$. Hence, $\dim(\mathrm{im}(T)) = 3$ in this case, and we have either $X \simeq \Omega^{-1} \oplus \Omega^{-1}$ or $X \simeq \Omega^{-2}$ (depending on whether $[N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)] \subseteq [\mathbb{Q}^\times]$).

The reader will notice that we have connected the solvability of particular embedding problems to the existence of certain points on rational conics $1 = by^2 - ax^2$. These are in turn connected to the splitting of quaternion algebras $(a, b)_{\mathbb{Q}}$ (see [18, Theorem 2.7]). However, this connection—and the well-established track record that the Brauer group has in encoding the solvability of certain Galois embedding problems (see [16, 17, 21, 22])—might suggest that there is something deeper to explore in this vein. Indeed, the solvability of each of the embedding problems

https://doi.org/10.4153/S0008414X22000165 Published online by Cambridge University Press

we have discussed is encoded in the vanishing of certain element(s) drawn from $\langle (a_1, a_1), (a_1, a_2), (a_2, a_2) \rangle \subseteq \mathrm{Br}(\mathbb{Q})$. The focus of the follow-up paper [9] is to reinterpret the decomposition of $J(K)$ provided by Theorem 1.1 through the lens of certain equations in $\mathrm{Br}(F)$. In particular, this will allow us to compute the multiplicities of the various summands by analyzing subspaces within $\mathrm{Br}(F)$, and ultimately show that all listed "unexceptional" summand types (i.e., $\mathbb{F}_2[\overline{G_i}]$ for $i \in \{0, 1, 2, 3, 4\}$, as well as Ω^1 and Ω^2) from Theorem 1.1 are realizable.

Acknowledgment We gratefully acknowledge discussions and collaborations with our friends and colleagues D. Benson, B. Brubaker, J. Carlson, S. Chebolu, I. Efrat, J. Gärtner, S. Gille, L. Heller, D. Hoffmann, J. Labute, T.-Y. Lam, R. Sharifi, N.D. Tan, A. Topaz, R. Vakil, K. Wickelgren, and O. Wittenberg, which have influenced our work in this and related papers. We are particularly grateful to A. Eimer and P. Guillot for their careful consideration of a previous draft of this manuscript which omitted Ω^2 summands. Finally, we are grateful for the careful attention that our manuscript received from two anonymous referees. The encouraging suggestions they made have helped improve both the expositional quality of the manuscript and its accuracy.

References

[1] A. Adem, W. Gao, D. Karagueuzian, and J. Mináč, *Field theory and the cohomology of some Galois groups*. J. Algebra **235**(2001), 608–635.
[2] A. Albert, *On cyclic fields*. Trans. Amer. Math. Soc. **37**(1935), no. 3, 454–462.
[3] D. Benson, *Representations and cohomology I*, Cambridge University Press, Cambridge, 1991.
[4] D. Benson, N. Lemire, J. Mináč, and J. Swallow, *Detecting pro-p groups that are not absolute Galois groups*. J. Reine Angew. Math. **613**(2007), 175–191.
[5] J. Berg and A. Schultz, *p-groups have unbounded realization multiplicity*. Proc. Amer. Math. Soc. **142**(2014), no. 7, 2281–2290.
[6] G. Bhandari, N. Lemire, J. Mináč, and J. Swallow, *Galois module structure of Milnor K-theory in characteristic p*. New York J. Math. **14**(2008), 215–224.
[7] Z. I. Borevič, *The multiplicative group of cyclic p-extensions of a local field*. Tr. Mat. Inst. Steklova **80**(1965), 16–29 (in Russian). English translation, Proc. Steklov Inst. Math. 80 (1965): *Algebraic number theory and representations*, edited by D. K. Faddeev, Providence, RI: American Mathematical Society, 1968, pp. 15–30.
[8] S. Chebolu, J. Mináč, and A. Schultz, *Galois p-groups and Galois modules*. Rocky Mountain J. Math. **46**(2016), 1405–1446.
[9] F. Chemotti, J. Mináč, T. T. Nguyen, A. Schultz, J. Swallow, and N. D. Tan, *Quaternion algebras and square power classes over biquadratic extensions*. Preprint, 2021. arXiv:2112.06688
[10] R. Dwilewicz, J. Mináč, A. Schultz, and J. Swallow, *Hilbert 90 for biquadratic extensions*. Amer. Math. Monthly **114**(2007), no. 7, 577–587.
[11] A. Eimer, *Modules of constant Jordan type from Galois extensions of local fields*. Preprint, 2021. arXiv:2006.15978
[12] D. K. Faddeev, *On the structure of the reduced multiplicative group of a cyclic extension of a local field*. Izv. Akad. Nauk SSSR Ser. Mat. **24**(1960), 145–152.
[13] J. Ferguson, The Galois cohomology of square-classes of units in Klein-four group extensions of characteristic not two, available at https://hdl.handle.net/10161/1276
[14] L. Heller, Galois module structure for Artin–Schreier theory over bicyclic extensions. Senior thesis, available at https://repository.wellesley.edu/object/ir734
[15] L. Heller, J. Mináč, T. T. Nguyen, A. Schultz, and N. D. Tan, *Galois module structure of some elementary p-abelian extensions*. Preprint, 2022. arxiv:2203.02604
[16] C. Jensen and N. Yui, *Quaternion extensions*. In: *Algebraic geometry and commutative algebra: in honor of Masayoshi Nagata*, Kinokuniya, Tokyo, 1987, pp. 155–182.
[17] I. Kiming, *Explicit classifications of some 2-extensions of a field of characteristic different from* 2. Canad. J. Math. **42**(1990), no. 5, 825–855.

[18] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, 67, American Mathematical Society, Providence, RI, 2005.
[19] N. Lemire, J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of Galois cohomology for embeddable cyclic extensions of degree p^n*. J. Lond. Math. Soc. (2) **81**(2010), no. 3, 525–543.
[20] N. Lemire, J. Mináč, and J. Swallow, *Galois module structure of Galois cohomology and partial Euler–Poincaré characteristics*. J. Reine Angew. Math. **613**(2007), 147–173.
[21] I. Michailov, *On Galois cohomology and realizability of 2-groups as Galois groups*. Cent. Eur. J. Math. **9**(2011), no. 2, 403–419.
[22] I. Michailov, *On Galois cohomology and realizability of 2-groups as Galois groups II*. Cent. Eur. J. Math. **9**(2011), no. 6, 1333–1343.
[23] J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of pth-power classes of cyclic extensions of degree p^n*. Proc. Lond. Math. Soc. (3) **92**(2006), 307–341.
[24] J. Mináč, A. Schultz, and J. Swallow, *Automatic realizations of Galois groups with cyclic quotient of order p^n*. J. Théor. Nombres Bordeaux **20**(2008), 419–430.
[25] J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of Milnor K-theory mod p^s in characteristic p*. New York J. Math. **14**(2008), 225–233.
[26] J. Mináč and J. Swallow, *Galois module structure of p th-power classes of extensions of degree p*. Israel J. Math. **138**(2003), 29–42.
[27] J. Mináč and J. Swallow, *Galois embedding problems with cyclic quotient of order p*. Israel J. Math. **145**(2005), 93–112.
[28] J. Mináč, J. Swallow, and A. Topaz, *Galois module structure of $\mathbb{Z}/\ell^n$ -th classes of fields*. Bull. Lond. Math. Soc. **46**(2014), no. 1, 143–154.
[29] A. Schultz, *Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p-abelian kernel*. J. Algebra **411**(2014), 50–91.
[30] A. Wadsworth, *Merkurjev's elementary proof of Merkurjev's theorem*. Contemp. Math. **55**(1986), no. II, 741–776.
[31] W. Waterhouse, *The normal closures of certain Kummer extensions*. Canad. Math. Bull. **37**(1994), no. 1, 133–139.

Bellevue, WA, USA
e-mail: fchemotti@gmail.com

Department of Mathematics, Western University, London, Ontario, Canada
e-mail: minac@uwo.ca

Department of Mathematics, Wellesley College, Wellesley, MA, USA
e-mail: andrew.c.schultz@gmail.com

Office of the President, Carthage College, Kenosha, WI, USA
e-mail: jswallow@carthage.edu