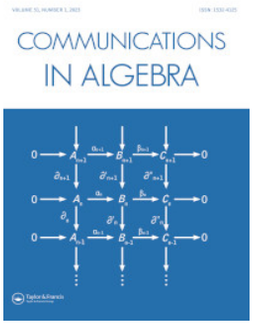
Taylor & Francis
Taylor & Francis Group



Communications in Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

A remark on a conjecture of Navarro and Tiep

Awildo Gutierrez, Yuqiao Huang, Nguyen Ngoc Hung, Duncan Peckham & Yong Yang

To cite this article: Awildo Gutierrez, Yuqiao Huang, Nguyen Ngoc Hung, Duncan Peckham & Yong Yang (2023) A remark on a conjecture of Navarro and Tiep, Communications in Algebra, 51:1, 150-156, DOI: 10.1080/00927872.2022.2092630

To link to this article: https://doi.org/10.1080/00927872.2022.2092630

Published online: 10 Jul 2022.

COMMUNICATIONS IN ALGEBRA®
2023, VOL. 51, NO. 1, 150–156
https://doi.org/10.1080/00927872.2022.2092630

Taylor & Francis
Taylor & Francis Group

A remark on a conjecture of Navarro and Tiep

Awildo Gutierrez[a], Yuqiao Huang[b], Nguyen Ngoc Hung[c], Duncan Peckham[d], and Yong Yang[e]

[a]Mathematics and Statistics Department, Hamilton College, Clinton, New York, USA; [b]Department of Mathematics, University of Rochester, Rochester, New York, USA; [c]Department of Mathematics, The University of Akron, Akron, Ohio, USA; [d]Department of Mathematics and Statistics, Boston University, Boston, Massachusetts, USA; [e]Department of Mathematics, Texas State University, San Marcos, Texas, USA

ABSTRACT

We prove a divisibility property of the fixed field in a cyclotomic field $\mathbb{Q}(e^{2i\pi/k})$ of the Frobenius automorphism $Gal(\mathbb{Q}(e^{2i\pi/k})/\mathbb{Q})\ni\tau:\xi\mapsto\xi^p$, where p is a prime, k is a positive integer relatively prime to p, and ξ is any k^{th}-root of unity. This implies that, for a finite group G, recent Navarro-Tiep's conjecture on fields of values of p'-degree irreducible characters of G follows from the celebrated Galois-McKay conjecture under a natural condition on p and the order of G.

ARTICLE HISTORY
Received 22 February 2022
Revised 18 May 2022
Communicated by Mandi Schaeffer Fry

KEYWORDS
Character values; Cyclotomic fields; Frobenius automorphisms; Galois-McKay conjecture

2020 MATHEMATICS SUBJECT CLASSIFICATION
Primary: 20C15; 12F10

1. Introduction

Let p be a prime, k a positive integer that is relatively prime to p, and $\mathbb{Q}_k := \mathbb{Q}(e^{2i\pi/k})$ denote the kth cyclotomic field. Let $\tau := \tau_{p,k} \in Gal(\mathbb{Q}_k/\mathbb{Q})$ denote the Frobenius automorphism $\xi \mapsto \xi^p$, where ξ is any k^{th}-root of unity. We write $\mathbb{F} := \mathbb{F}_{p,k}$ for the fixed field in $\mathbb{Q}_k$ of τ

The field $\mathbb{F}$ arises naturally in the representation theory of finite groups, in particular in the context of the celebrated Galois-McKay conjecture, see [7] and [8, Conjecture 7.6]. Loosely speaking, for a finite group G and a prime p, the conjecture predicts that there is a bijection between the set of the (complex) irreducible characters of degree not divisible by p of G and that of a p-local subgroup of G such that the fields of values of corresponding characters are the same up to $\mathbb{F}_{p,|G|_{p'}}$, where $|G|_{p'}$ is the p'-part of $|G|$. (See Section 2 for details.)

In the following, $\text{ord}_k(p)$ is the multiplicative order of p modulo k, φ is Euler's phi function, and the conductor of an abelian extension E of $\mathbb{Q}$, denoted by $c(E)$, is the smallest positive integer n such that $E \subseteq \mathbb{Q}_n$.

Theorem 1.1. *Let p be a prime and k a positive integer coprime to p. Let E be an abelian extension of $\mathbb{Q}$ such that $E \subseteq \mathbb{Q}_{p^a k}$ and $p^a | c(E)$ for some $a \in \mathbb{Z}^{\geq 0}$. Suppose that p does not divide $\varphi(k)/\text{ord}_k(p)$. Then p does not divide $[(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})]$.*

CONTACT Yong Yang yang@txstate.edu Department of Mathematics, Texas State University, San Marcos, TX 78666, USA.

Inspired by the aforementioned Galois-McKay conjecture, there has been a growing interest in the study of fields of values of irreducible characters of degree not divisible by a given prime. For instance, following up the work of Isaacs, Liebeck, Navarro, and Tiep [2] on fields of values of odd-degree irreducible characters, the latter two authors [9] recently attempted to classify all the abelian extensions of rational numbers that could be the field of values of an irreducible character of degree not divisible by p. They conjectured that, for an irreducible complex character χ of degree not divisible by p of a finite group G with $c(\mathbb{Q}(\chi)) = p^a m$, where $(p, m) = 1$ and $a \in \mathbb{Z}^{\geq 0}$, the degree $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})]$ is not divisible by p. (See [9, Theorem B1 and Conjecture B3]. Recall that $\mathbb{Q}(\chi)$ is the field of values of χ, which is defined to be the smallest field containing all the values of χ.)

Theorem 1.1 implies the following.

Theorem 1.2. *Let G be a finite group of order p^{bk}, where p is a prime and k a positive integer coprime to p. Suppose that p does not divide $\varphi(k)/\mathrm{ord}_k(p)$. Then Navarro-Tiep's conjecture follows from the Galois-McKay conjecture for G and p.*

We remark that the hypothesis on p cannot be removed, at least in Theorem 1.1 (see Examples 3.6). It is not difficult to see that p does not divide $\varphi(k)/\mathrm{ord}_k(p)$ if k has no prime divisor q such that $p|(q-1)$, and therefore the condition has higher chance to be satisfied when p is larger. In Proposition 4.2, we will describe exactly when this condition is fulfilled.

2. The Galois-McKay conjecture and Navarro-Tiep's conjecture

Let G be a finite group and p a prime. Let P be a Sylow p-subgroup of G. The well-known McKay conjecture [6] asserts that the number of irreducible ordinary characters of p'-degree of G is equal to that of the normalizer $\mathbf{N}_G(P)$ of P in G. That is,

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|,$$

where $\mathrm{Irr}_{p'}(G)$, as usual, denotes the set of irreducible characters of p'-degree of G. In spite of the considerable effort of many researchers over the past two decades (see [3, 5] and subsequent papers), the conjecture is still unsolved and a correct form of a canonical bijection between the two sets $\mathrm{Irr}_{p'}(G)$ and $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ for general G and p remains to be found.

In the landmark paper [7], Navarro proposed that there should be a bijection from $\mathrm{Irr}_{p'}(G)$ to $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ that commutes with the action of a certain subgroup of the Galois group $\mathcal{G} := Gal(\mathbb{Q}_{|G|}/\mathbb{Q})$. This subgroup is

$$\mathcal{H} := \{\sigma \in \mathcal{G} \,|\, \exists n \in \mathbb{Z}^{\geq 0} \text{ s.t. for any p'th} - \text{root } \xi \text{ of unity, } \sigma(\xi) = \xi^{p^n}\}.$$

Navarro's remarkable refinement of the McKay conjecture, often referred to as the Galois-McKay conjecture, offers that there is a similarity between the fields of values of characters in $\mathrm{Irr}_{p'}(G)$ and $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$. An equivalent form of the conjecture is the following, see [9, p. 23].

Conjecture 2.1 (Galois-McKay). *Let G be a finite group and p a prime. Let P be a Sylow p-subgroup of G. There exists a bijection*

$$* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$$

such that

$$\mathbb{F}(\chi) = \mathbb{F}(\chi^*)$$

for every $\chi \in \mathrm{Irr}_{p'}(G)$.

We recall that $\mathbb{F}(\chi)$ is the smallest field containing $\mathbb{F}$ and all the values of χ. The conjecture basically claims that the p'-degree irreducible characters of G and $\mathbf{N}_G(P)$ have similar fields of values up to $\mathbb{F}$, where $\mathbb{F}$ is the fixed field of $\mathcal{H}$ in $\mathbb{Q}_{|G|}$. If $|G|_{p'} = k$, $\mathbb{F}$ is the same as the fixed field in $\mathbb{Q}_k$ of the Frobenius automorphism mentioned in the introduction.

Although the Galois-McKay conjecture proposes a way to determine possible abelian extensions $\mathbb{F}(\chi)$ for $\chi \in \mathrm{Irr}_{p'}(G)$ via the normalizer $\mathbf{N}_G(P)$, it does not directly tell us what the fields of values $\mathbb{Q}(\chi)$ are for $\chi \in \mathrm{Irr}_{p'}(G)$.

Partly motivated by the Galois-McKay conjecture, there has been growing interest in the study of fields of character values, especially of those characters of p'-degree. For instance, in [2], Isaacs, Liebeck, Navarro, and Tiep proved that, if $\chi \in \mathrm{Irr}_{2'}(G)$, then either $\sqrt{-1} \in \mathbb{Q}(\chi)$ or $\mathbb{Q}(\chi)$ is contained in $\mathbb{Q}_n$ for some odd integer n. Extending this result, Navarro and Tiep studied the problem of determining all the possible fields of values of p'-degree irreducible characters of finite groups. It is conjectured in [9] that, for a field E with $c(E) = p^a m$ where $(p, m) = 1$ and $a \in \mathbb{Z}^{\geq 0}$, E is the field of values of a p'-degree irreducible character of a finite group if and only if $[\mathbb{Q}_{p^a} : (E \cap \mathbb{Q}_{p^a})]$ is not divisible by p. In fact, they managed to confirm the "if" implication for all p and both implications for $p = 2$. The "only if" part, which is stated below, turns out to be the deeper one of the conjecture.

Conjecture 2.2 (Navarro-Tiep). *Let p be a prime. Let G be a finite group and $\chi \in \mathrm{Irr}_{p'}(G)$ such that $c(\mathbb{Q}(\chi)) = p^a m$ where $(p, m) = 1$ and $a \in \mathbb{Z}^{\geq 0}$. Then $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})]$ is not divisible by p.*

One of the purposes of the present note is to find conditions on p and $|G|$ in which Navarro-Tiep's conjecture follows from the Galois-McKay conjecture.

3. The fixed field $\mathbb{F}$

Let n be a positive integer and suppose $n = p^b k$ where p is a prime, $b \in \mathbb{Z}^{\geq 0}$, $k \in \mathbb{Z}^{>0}$, and $p \nmid k$. Recall from the previous section that $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}_n^\times$ and $\mathcal{H}$ is the subgroup of $\mathcal{G}$ consisting of those automorphisms that send p'th-root of unity to some arbitrary but fixed p-power. Also, the fixed field of $\mathcal{H}$ in $\mathbb{Q}_n$ is $\mathbb{F} = \mathrm{Fix}(\mathcal{H})$. Recall also that $\mathrm{ord}_k(p)$ is the multiplicative order of p modulo k and φ is Euler's phi function.

Lemma 3.1. *Suppose the above notation. We have $|\mathbb{F} : \mathbb{Q}| = \frac{\varphi(k)}{\mathrm{ord}_k(p)}$ and $|\mathbb{Q}_k : \mathbb{F}| = \mathrm{ord}_k(p)$.*

Proof. We have $[\mathbb{F} : \mathbb{Q}] = [\mathrm{Fix}(\mathcal{H}) : \mathbb{Q}] = |\mathrm{Gal}(\mathrm{Fix}(\mathcal{H})/\mathbb{Q})|$ where

$$\mathrm{Gal}(\mathrm{Fix}(\mathcal{H})/\mathbb{Q}) \cong \mathcal{G}/\mathrm{Gal}(\mathbb{Q}_n/\mathrm{Fix}(\mathcal{H})) = \mathcal{G}/\mathcal{H}.$$

Therefore $|\mathrm{Fix}(\mathcal{H}) : \mathbb{Q}| = |\mathcal{G} : \mathcal{H}|$. The fact that $|\mathcal{G} : \mathcal{H}| = \frac{\varphi(k)}{\mathrm{ord}_k(p)}$ follows from the description of $\mathcal{H}$. The second conclusion of the lemma immediately follows from the first. □

One can determine exactly when $\mathbb{F} = \mathbb{Q}$. By the fundamental theorem of Galois theory, $\mathrm{Fix}(\mathcal{H}) = \mathbb{Q}$ if and only if $\mathcal{H} = \mathcal{G}$, which happens if and only if p is a generator for $\mathbb{Z}/k\mathbb{Z}$. It is known that $\mathbb{Z}_k^\times$ is cyclic if and only if $k = 1, 2, 4, q^l$, or $2q^l$ where q is an odd prime and $l \in \mathbb{N}$. Furthermore, given generators of $\mathbb{Z}_q^\times$, one can construct all generators of $\mathbb{Z}_{q^l}^\times$ for any $l \in \mathbb{N}$, see [4, Lemma 4 and Theorem 1].

We now prove a critical result that is needed in the proofs of Theorems 1.1 and 1.2.

Theorem 3.2. *Let p be a prime and k a positive integer coprime to p. Let $\mathbb{F}$ be the fixed field in $\mathbb{Q}_k$ of the Frobenius automorphism τ and $a \in \mathbb{Z}^{\geq 0}$. Assume that p does not divide $[\mathbb{F} : \mathbb{Q}]$. Then $[(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})]$ is not divisible by p for every field $E \subseteq \mathbb{Q}_{p^a k}$ such that $p^a | c(E)$.*

Proof. We have

$$\begin{aligned}&|\mathbb{F}E : (\mathbb{F}E \cap \mathbb{Q}_{p^a})||(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})|\\ &= |\mathbb{F}E : (E \cap \mathbb{Q}_{p^a})|\\ &= |\mathbb{F}E : E||E : (E \cap \mathbb{Q}_{p^a})|\\ &= |\mathbb{F} : (\mathbb{F} \cap E)||E : (E \cap \mathbb{Q}_{p^a})|.\end{aligned}$$

Note that $|\mathbb{F}E : (\mathbb{F}E \cap \mathbb{Q}_{p^a})| = |\mathbb{F}E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}|$ and $|E : (E \cap \mathbb{Q}_{p^a})| = |E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}|$. Thus we have

$$|\mathbb{F}E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}||(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})| = |\mathbb{F} : (\mathbb{F} \cap E)||E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}|.$$

It follows that

$$\frac{|\mathbb{F}E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}|}{|E\mathbb{Q}_{p^a} : \mathbb{Q}_{p^a}|}|(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})| = |\mathbb{F} : (\mathbb{F} \cap E)|,$$

and therefore

$$|\mathbb{F}E\mathbb{Q}_{p^a} : E\mathbb{Q}_{p^a}||(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})| = |\mathbb{F} : (\mathbb{F} \cap E)|.$$

Since $|\mathbb{F} : \mathbb{F} \cap E|$ divides $|\mathbb{F} : \mathbb{Q}|$, which is not divisible by p, the result follows. □

Theorem 1.1 now follows from Theorem 3.2 and Lemma 3.1.

It is worth noting that there are cases where p does divide $|(\mathbb{F}E \cap \mathbb{Q}_{p^a}) : (E \cap \mathbb{Q}_{p^a})|$. To provide an example, we describe the field $\mathbb{F}$ as an extension of $\mathbb{Q}$ by certain elements associated to a primitive kth of unity.

Now, let $o := \mathrm{ord}_k(p)$, $m := \frac{\varphi(k)}{o}$, and ζ a primitive kth root of unity. By basic properties of Galois extension,

$$\min_{\mathbb{F}}(\zeta) = (x-\zeta)(x-\zeta^p)(x-\zeta^{p^2})\cdots(x-\zeta^{p^{o-1}}),$$

where $\{\zeta, \zeta^p, ..., \zeta^{p^{o-1}}\}$ form the orbit of ζ under $\mathrm{Gal}(\mathbb{Q}_k/\mathbb{F})$, and $\min_{\mathbb{F}}(\zeta)$ is the minimal polynomial of ζ over $\mathbb{F}$. Let e_i denote the coefficient of x^i in $\min_{\mathbb{F}}(\zeta)$ for $i = 0, ..., o-1$.

Theorem 3.3. *Suppose that k is square-free. Then $\mathbb{F} = \mathbb{Q}(\zeta + \zeta^p + \cdots + \zeta^{p^{o-1}})$ where $o := ord_k(p)$ and ζ a primitive kth root of unity.*

Proof. Let $\alpha := \zeta + \zeta^p + \cdots + \zeta^{p^{o-1}}$. We show that α is a primitive element for the extension $\mathbb{F}$ over $\mathbb{Q}$. For j coprime to k, let $\tau_j \in \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})$ be the automorphism $\zeta \mapsto \zeta^j$, and let

$$\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})/\langle\tau_p\rangle = \{\tau_{j_1}\langle\tau_p\rangle, \tau_{j_2}\langle\tau_p\rangle, ..., \tau_{j_m}\langle\tau_p\rangle\}$$

where $j_1 = 1$, and therefore τ_{j_1} is the identity function.

It is known that, when k is square-free, the set of all primitive k^{th}-roots of unity form a normal basis for $\mathbb{Q}_k$ over $\mathbb{Q}$ [1, Example 3.2]. Consider

$$\begin{aligned}\tau_{j_1}(\alpha) &= \zeta + \zeta^p + \cdots + \zeta^{p^{n-1}},\\ \tau_{j_2}(\alpha) &= \zeta^{j_2} + \zeta^{j_2 p} + \cdots + \zeta^{j_2 p^{n-1}},\\ &\cdots\\ \tau_{j_m}(\alpha) &= \zeta^{j_m} + \zeta^{j_m p} + \cdots + \zeta^{j_m p^{o-1}},\end{aligned}$$

in which the summands are exactly the primitive k^{th}-roots of unity. Thus the sums must all be distinct. Otherwise, it would contradict the linear independence of primitive k^{th}-roots of 1.

Therefore $|\mathcal{O}(\alpha)| = m$ where $\mathcal{O}(\alpha)$ denotes the orbit of α under the action of $\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})$. Hence $\mathrm{degmin}_{\mathbb{Q}}(\alpha) = m$ and we conclude $\mathbb{F} = \mathbb{Q}(\alpha)$ as $|\mathbb{F} : \mathbb{Q}| = m$ by Lemma 3.1. □

Remark 3.4. When k is not square-free, α sometimes fails to be a primitive element. For instance, let $p = 5, k = 8$, then we have $\alpha = \zeta + \zeta^5 = 0$ but $o = 2 = m$. However, in this case, the free coefficient $e_0 = \zeta \cdot \zeta^5 = -i$ is indeed a primitive element.

The element α in the above proof is precisely $-e_{o-1}$, where e_{o-1} is the coefficient of x^{o-1} in the polynomial $\min_{\mathbb{F}}(\zeta)$. Therefore, Theorem 3.3 simply states that $\mathbb{F} = \mathbb{Q}(e_{o-1})$ when k is square-free. For arbitrary k, we have:

Theorem 3.5. *Let e_i be the coefficient of x^i in $\min_{\mathbb{F}}(\zeta)$, for $i = 0, \ldots, o-1$. Then $\mathbb{F} = \mathbb{Q}(e_{o-1}, \ldots, e_0)$.*

Proof. We prove a more general statement that, if $F \subseteq K \subseteq F(\alpha)$ are fields where α is algebraic over F, and $\min_K(\alpha) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ where $n \in \mathbb{N}$ and $c_i \in K$ for $i = 0, \ldots, n-1$, then $K = F(c_{n-1}, \ldots, c_0)$.

Let $L := F(c_{n-1}, \ldots, c_0)$. Notice that $L \subseteq K$. Let $f := \min_K(\alpha)$ and $g := \min_L(\alpha)$. We have $f|g$ in $K[x]$ since $g \in K[x]$ and $g(\alpha) = 0$. Also, we have $g|f$ in $L[x]$ since $f \in L[x]$ and $f(\alpha) = 0$, which implies $g|f$ in $K[x]$ as $L[x] \subseteq K[x]$. Therefore $g = f$.

As $L(\alpha) = F(\alpha) = K(\alpha)$, we have

$$|F(\alpha) : L| = |L(\alpha) : L| = \deg g = \deg f = |K(\alpha) : K| = |F(\alpha) : K|.$$

Hence $|K : L| = 1$ and $K = L$, as wanted. □

Example 3.6. Take $p = 2, k = 7, a = 2, \zeta_7 = e^{\frac{2\pi}{7}i}$, so $\varphi(k) = 6, o = 3, m = 2$. By Theorem 3.3, $\mathbb{F} = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) = \mathbb{Q}\left(i\sqrt{7}\right) \subseteq \mathbb{Q}_7$. Let $E := \mathbb{Q}\left(\sqrt{7}\right) \subseteq \mathbb{Q}_{28}$, and indeed $c(E) = 28$. We have $\mathbb{Q}_4 \subseteq \mathbb{F}E$ but $\mathbb{Q}_4 \not\subseteq E$. Hence $|(\mathbb{F}E \cap \mathbb{Q}_4) : (E \cap \mathbb{Q}_4)| = |\mathbb{Q}_4 : \mathbb{Q}| = 2 = p$.

4. Proof of Theorem 1.2

We now deduce Theorem 1.2 from Theorem 1.1.

Theorem 4.1. *Let G be a finite group of order p^{bk}, where p is a prime and k a positive integer coprime to p. Suppose that p does not divide $\varphi(k)/\mathrm{ord}_k(p)$. Then Navarro-Tiep's conjecture follows from the Galois-McKay conjecture for G and p.*

Proof. Let $\chi \in \mathrm{Irr}_{p'}(G)$ and assume that $c(\mathbb{Q}(\chi)) = p^a m$, where $(p, m) = 1$. Since $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{|G|}$, we have $m|k$ and $a \leq b$. Suppose that the Galois-McKay conjecture holds for G and p. We would like to show that $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})]$ is not divisible by p.

We have $\mathbb{F}(\chi) = \mathbb{F}(\chi^*)$ for some χ^* in $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$, where P is a Sylow p-subgroup of G and $\mathbb{F}$ is the fixed field in $\mathbb{Q}_k$ of the Frobenius automorphism $\xi \mapsto \xi^p$. Note that the conductor of $\mathbb{Q}(\chi^*)$ is $p^a m_1$ for some m_1 relatively to p. It follows by [9, Lemmas 7.1 and 7.3] that $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi^*) \cap \mathbb{Q}_{p^a})]$ is not divisible by p. Therefore,

$$p \nmid \left[\mathbb{Q}_{p^a} : (\mathbb{F}(\chi^*) \cap \mathbb{Q}_{p^a})\right],$$

and so

$$p \nmid \left[\mathbb{Q}_{p^a} : (\mathbb{F}(\chi) \cap \mathbb{Q}_{p^a})\right].$$

Now using Theorem 3.2 with $\mathbb{Q}(\chi)$ in place of E and note from Lemma 3.1 that $[\mathbb{F} : \mathbb{Q}] = \varphi(k)/\mathrm{ord}_k(p)$, we have

$$p \nmid \left[(\mathbb{F}(\chi) \cap \mathbb{Q}_{p^a}) : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})\right].$$

The last two displayed statements imply that $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})]$ is not divisible by p, as desired. □

We now describe the situations where the hypothesis of Theorems 1.1 and 1.2 are satisfied.

Proposition 4.2. *Let p be a prime and k a positive integer coprime to p. Then p does not divide $\varphi(k)/\mathrm{ord}_k(p)$ if and only if one of the following holds:*

i. *k has no prime divisor q such that $p|(q-1)$,*
ii. *k has a unique prime divisor q such that $p|(q-1)$. Additionally, q does not divide $p^{(q-1)/p}-1$.*

Proof. We use n_p to denote the p-part of n and $\nu(n) := \nu_p(n) = \log_p(n_p)$ the p-adic valuation of n. Let $k = \Pi q_i^{a_i}$ be the prime factorization of k, where q_is are distinct. Recall that $\varphi(k) = k\Pi_i\left(1-\frac{1}{q_i}\right)$. Therefore,

$$\nu(\varphi(k)) = \sum_i \nu(q_i - 1).$$

On the other hand, since $\mathrm{ord}_k(p) = \mathrm{lcm}\{\mathrm{ord}_{q_i}(p) : i = 1, 2, \ldots\}$ and $\mathrm{ord}_{q_i}(p) | q_i^{a_i - 1}(q_i - 1)$, we have

$$\nu(\mathrm{ord}_k(p)) \leq \max_i\{\nu(q_i - 1)\}.$$

The last two displayed formulas immediately imply that if p divides no $q_i - 1$ then $p \nmid \varphi(k)/\mathrm{ord}_k(p)$ and if p divides more than one $q_i - 1$ then $p|\varphi(k)/\mathrm{ord}_k(p)$. Thus we may now assume that there is a unique prime divisor q of k such that $p|(q-1)$.

Let $a := \log_q(k_q) \geq 1$. Then, as analyzed above, p does not divide $\varphi(k)/\mathrm{ord}_k(p)$ if and only if $\nu(q-1) = \nu(\mathrm{ord}_{q^a}(p))$. But $\nu(\mathrm{ord}_{q^a}(p)) = \nu(\mathrm{ord}_q(p))$ (this is because $\mathrm{ord}_q(p) | \mathrm{ord}_{q^a}(p)$ and $\mathrm{ord}_{q^{x+1}}(p) | q \cdot \mathrm{ord}_{q^x}(p)$ for every $x \in \mathbb{Z}^+$), and so p does not divide $\varphi(k)/\mathrm{ord}_k(p)$ if and only if $\nu(q-1) = \nu(\mathrm{ord}_q(p))$. This happens if and only if q does not divide $p^{(q-1)/p} - 1$, as stated. □

Acknowledgements

The authors gratefully acknowledge the financial support of NSF and NSA, and also thank Texas State University for providing a great working environment and support. Finally, we are grateful to the referee for several constructive suggestions that have greatly improved the exposition in the paper.

Funding

This research was conducted under NSF-REU grant DMS-1757233 and NSA grant H98230-21-1-0333 by Gutierrez, Huang, and Peckham during the summer of 2021 under the supervision of Hung and Yang. Yang was also partially supported by a grant from the Simons Foundation (#499532, YY).

References

[1] Conrad, K. (2008). Linear independence of characters. kconrad.math.uconn.edu/blurbs/galoistheory/linearchar.pdf.

[2] Isaacs, I. M., Liebeck, M. W., Navarro, G., Tiep, P. H. (2019). Fields of values of odd-degree irreducible characters. *Adv. Math*. 354(1):106757. DOI: 10.1016/j.aim.2019.106757.
[3] Isaacs, I. M., Malle, G., Navarro, G. (2007). A reduction theorem for the McKay conjecture. *Invent. Math*. 170(1):33–101. DOI: 10.1007/s00222-007-0057-y.
[4] Jolly, N. (2008). Constructing the primitive roots of prime powers. Honors thesis. Monash University, Australia.
[5] Malle, B., Späth, B. (2016). Characters of odd degree. *Ann. Math*. 184(3):869–908. DOI: 10.4007/annals.2016.184.3.6.
[6] McKay, J. (1972). Irreducible representations of odd degree. *J. Algebra* 20(2):416–418. DOI: 10.1016/0021-8693(72)90066-X.
[7] Navarro, G. (2004). The McKay conjecture and Galois automorphisms. *Ann. Math*. 160(3):1129–1140. DOI: 10.4007/annals.2004.160.1129.
[8] Navarro, G. (2018). *Character Theory and the McKay Conjecture*. Cambridge: Cambridge Studies in Advanced Mathematics 175, Cambridge University Press.
[9] Navarro, G., Tiep, P. H. (2021). The fields of values of characters of degree not divisible by *p*. *Forum Math. Pi*. 9e2:1–28.