www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 4 No. 1 (2015), pp. 1-6.

www.ui.ac.ir

COMPUTING CHARACTER DEGREES VIA A GALOIS CONNECTION

MARK L. LEWIS* AND JOHN K. MCVEY

Communicated by Patrizia Longobardi

Abstract. In a previous paper, the second author established that, given finite fields $F < E$ and certain subgroups $C \leq E^\times$, there is a Galois connection between the intermediate field lattice $\{L \mid F \leq L \leq E\}$ and C's subgroup lattice. Based on the Galois connection, the paper then calculated the irreducible, complex character degrees of the semi-direct product $C \rtimes \mathrm{Gal}(E/F)$. However, the analysis when $|F|$ is a Mersenne prime is more complicated, so certain cases were omitted from that paper.

The present exposition, which is a reworking of the previous article, provides a uniform analysis over all the families, including the previously undetermined ones. In the group $C \rtimes \mathrm{Gal(E/F)}$, we use the Galois connection to calculate stabilizers of linear characters, and these stabilizers determine the full character degree set. This is shown for each subgroup $C \leq E^\times$ which satisfies the condition that every prime dividing $|E^\times : C|$ divides $|F^\times|$.

1. Introduction

In this note, we consider a situation that often arises when studying the degrees of the irreducible characters of an arbitrary finite group. One can often reduce a problem of interest to studying a group H which is the split extension of a finite group G acting faithfully and primitively on a finite, irreducible module V. One of the main cases that arises in this situation is when G is a subgroup of the semi-linear group $\Gamma(V)$ of V (see for example Corollary 2.3 and Theorem 2.11 in [2]). When this happens, V is an elementary abelian p-group for some prime p and rank e, and can be identified as the additive group of a field E of order p^e. Under this identification, $\Gamma(V) = \{x \mapsto ax^\sigma \mid a \in E^\times, \sigma \in \mathrm{Gal}(E/\mathbb{F}_p)\}$ where $E^\times$ is the multiplicative group of E and $\mathrm{Gal}(E/\mathbb{F}_p)$ is the Galois group of E with respect to its prime

MSC(2010): Primary 20C15; Secondary 06A15.

Keywords: Galois correspondence; lattice; character degree; finite field.

Received: 9 June 2014, Accepted: 3 September 2014.

*Corresponding author.

subfield $\mathbb{F}_p$. It is not difficult to see that $\Gamma(V)$ has the form $E^\times \rtimes \mathrm{Gal}(G/\mathbb{F}_p)$. Our goal is to compute the set of character degrees $\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$ for certain subgroups G of $\Gamma(V)$ and where $\mathrm{Irr}(G)$ is the set of irreducible characters of G.

In the papers [3] and [4], which generalize results in §5 of [5], the second author worked on determining character degree sets for groups of the form $G = C \rtimes \mathrm{Gal}(E/F)$ where $F < E$ are finite fields of order $q < q^e$, respectively, and where $C < E^\times$. In Theorem 3.2 of [3], the second author proved when $\gcd(q-1, e) = 1$ and $|C| = (q^e - 1)/(q-1)$ that $\mathrm{cd}(G) = \{n \mid n \text{ divides } e\}$. In [4], the second author weakened the condition that $q-1$ and e be relatively prime to the condition that $C \leq E^\times$ has index $|E^\times : C|$ which is divisible only by primes that divide $|F^\times|$. In Theorem 5 of [4], it was proved that $\mathrm{cd}(G)$ is the full list of divisors of $|E : F|$, except possibly when three conditions are mutually satisfied: (i) $|F|$ is a Mersenne prime, (ii) the degree $|E : F|$ is even, and (iii) 4 does not divide $|C|$. However, the character degree set for G when these conditions were mutually satisfied remained unspecified. The intent of this article is to provide a uniform analysis over all cases, including when (i)–(iii) hold. In particular, we show that the corresponding character degree set is the full list of divisors of $|E : F|$, but with the integer 2 removed when (i)–(iii) simultaneously hold.

In particular, we will prove the following result:

Theorem 1.1. *Fix a prime-power q and an exponent $1 < e \in \mathbb{Z}$, and label by F the field $\mathbb{F}_q$, by E the field $\mathbb{F}_{q^e}$, and by π the set of primes dividing $q-1$. Let $\Gamma = \mathrm{Gal}(E/F)$, and fix $C \leq E^\times$ under the assumption $|E^\times : C|$ is a π-number. Let $G = C \rtimes \Gamma$. If all three of the following conditions are satisfied*

(i) *q is Mersenne,*
(ii) *e is even, and*
(iii) *4 does not divide $|C|$,*

then

$$\mathrm{cd}(G) = \{n \mid n \text{ divides } e\} \setminus \{2\}.$$

If any of these conditions is violated, then

$$\mathrm{cd}(G) = \{n \mid n \text{ divides } e\}.$$

2. The Galois Connection

In this section, we review the results on *monotone* Galois connections that were proved in Section 2 of [4]. Since these results are fundamental to our argument, we provide a thorough review of the results. We refer the interested reader to [4] for the proofs of these results.

A monotone Galois connection is a pair of monotone nondecreasing functions $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{B} \to \mathcal{A}$ on partially ordered sets $(\mathcal{A}, \leq)$ and $(\mathcal{B}, \leq)$ which satisfy

$$f(a) \leq b \text{ if and only if } a \leq g(b)$$

over all $a \in \mathcal{A}$ and $b \in \mathcal{B}$. The *lower* and *upper adjoints* are f and g respectively. The *closed sets* $\mathcal{A}_0$ and $\mathcal{B}_0$ of $\mathcal{A}$ and $\mathcal{B}$ respectively are defined by $\mathcal{A}_0 = g(\mathcal{B})$ and $\mathcal{B}_0 = f(\mathcal{A})$, and satisfy

$$\mathcal{A}_0 = \{a \in \mathcal{A} \mid g \circ f(a) = a\} = g \circ f(\mathcal{A}) \text{ and}$$

$$\mathcal{B}_0 = \{b \in \mathcal{B} \mid f \circ g(b) = b\} = f \circ g(\mathcal{B}).$$

The functions f and g are inverse bijections between the sets $\mathcal{A}_0$ and $\mathcal{B}_0$.

We now focus our attention specifically on finite fields $F < E$. Label by π the set of primes dividing $|F^\times| = |F|-1$ and consider an arbitrary subgroup $C \leq E^\times$ for which the index $|E^\times : C|$ is a π-number.[1] In this notation, the upper adjoint in which we are interested is the function "intersect with C."

As to the lower adjoint, define the *F-closure* $\widehat{X}$ of a subset $X \subseteq E$ to be the smallest subfield of E which contains $X \cup F$. In other words, $\widehat{X}$ is the intersection of all fields L satisfying $X \cup F \subseteq L \leq E$. Obviously, this actually is a closure operator, i.e.

$$X \subseteq Y \text{ implies } \widehat{X} \subseteq \widehat{Y} \text{ and } X \subseteq \widehat{X} = \widehat{\widehat{X}}$$

over all subsets $X, Y \subseteq E$. Most importantly, an automorphism $\sigma \in \mathrm{Gal}(E/F)$ centralizes X if and only if it centralizes $\widehat{X}$. The partially ordered sets are

$$\mathcal{E} = \{L \mid F \leq L \leq E\} \text{ and } \mathcal{C} = \{D \mid D \leq C\}$$

under inclusion. The functions $X \longmapsto X \cap C$ and $X \longmapsto \widehat{X}$ are certainly both monotone.

Given $D \in \mathcal{C}$ and $L \in \mathcal{E}$, and noting $L \cap C = L^\times \cap C \in \mathcal{C}$,

$$\widehat{D} \subseteq L \text{ if and only if } D \subseteq L \text{ if and only if } D \subseteq L \cap C,$$

showing $\widehat{\cdot}$ and $(\,\cdot\,) \cap C$ are lower and upper adjoints, respectively. Therefore, as $\mathcal{A}_0 = g(\mathcal{B})$, the closed subset of $\mathcal{C}$ is $\mathcal{C}_0 = \{L \cap C \mid L \in \mathcal{E}\}$.

We are now ready to collect our results on the Galois connection. All but the last two sentences were proven in the above discussion, those being the true content of the theorem. Their proof is at the end of this section. This result is the Main Theorem from [4].

Theorem 2.1. *Let $F < E$ be finite fields and label by π the set of primes dividing $|F| - 1$. Let C be a subgroup of $E^\times$ whose index $|E^\times : C|$ is a π-number. Given the partially ordered sets*

$$\mathcal{E} = \{L \mid F \leq L \leq E \textit{ is a field}\} \textit{ and}$$

$$\mathcal{C} = \{D \mid D \leq C \textit{ is a group}\},$$

the functions $\widehat{\cdot} : \mathcal{C} \to \mathcal{E}$ and $(\cdot) \cap C : \mathcal{E} \to \mathcal{C}$ are respectively the lower and upper adjoints of a monotone Galois connection, and thus provide inverse bijections between the closed subsets $\mathcal{C}_0 \subseteq \mathcal{C}$ and $\mathcal{E}_0 \subseteq \mathcal{E}$. The closed subset $\mathcal{C}_0$ of $\mathcal{C}$ is the lattice $\mathcal{C}_0 = \{L \cap C \mid L \in \mathcal{E}\}$. If $|F|$ is a Mersenne prime, $|E : F|$ is even, and 4 does not divide $|C|$, then the closed subset $\mathcal{E}_0$ of $\mathcal{E}$ is the set $\mathcal{E}_0 = \mathcal{E} \setminus \{K\}$ where $|K : F| = 2$. Otherwise, $\mathcal{E} = \mathcal{E}_0$.

[1] This naturally generalizes [5], wherein $|E^\times : C| = |F^\times|$.

Our argument for the unfinished portion relies on number theory, for which we quote Zsigmondy's prime theorem (see [6]).

Theorem 2.2 (Zsigmondy)**.** *Let a, b, n be positive integers and assume a, b are coprime and not both 1. Then, $a^n - b^n$ has a prime divisor which does not divide $a^k - b^k$ for integers $0 < k < n$, except when either*

- *$n = 6$ and $\{a, b\} = \{1, 2\}$, or*
- *$n = 2$ and $a + b$ is a 2-power.*

For our application, we need to be both a bit more specific (in one direction) and a bit more general (in another) than Zsigmondy's theorem. In Corollary 2.3, we specify that $\{a, b\}$ be $\{q, 1\}$ with q a prime-power, but we also generalize by switching the order of the quantifiers (from '$\exists$ prime $\forall\, k$' in Zsigmondy's theorem to '$\forall\, k$ $\exists$ prime' in the corollary). We quote directly Corollary 2 of [4].

Corollary 2.3. *Let $n > 1$ be an integer and q a power of a prime. Then, for each integer k with $0 < k < n$, there is a prime which divides $q^n - 1$ and not $q^k - 1$, except when q is a Mersenne prime and $n = 2$. Conversely, when q is a Mersenne prime, every prime dividing $q^2 - 1$ divides $q - 1$.*

We leave number theory and move to algebra proper. Our first algebraic lemma applies the above number theory to finite fields. This result previously appeared as Lemma 3 in [4].

Lemma 2.4. *Let $F \leq K \leq L \leq E$ be finite fields. For the set π of prime divisors of $|F^\times|$, let C be a subgroup of $E^\times$ whose index is a π-number. If the prime p divides $|L^\times|$ and not $|K^\times|$, then p divides $|L \cap C : K \cap C|$.*

We now make the last of our direct quotes; the following theorem appeared as Theorem 4 in [4]. As a direct consequence of this theorem and the statement that $\mathcal{B}_0 = f \circ g(\mathcal{B})$, we conclude

$$\mathcal{E}_0 = \left\{ \widehat{L \cap C} \,\middle|\, L \in \mathcal{E} \right\}.$$

Since the F-closure $\widehat{L \cap C}$ equals L but for the one exception $\mathbb{F}_{q^2}$ when q is Mersenne, e is even, and 4 fails to divide $|C|$, this finishes the proof of Theorem 2.1.

Theorem 2.5. *Let q be a prime-power, $e > 1$ an integer, and π the set of primes dividing $q - 1$. Label $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^e}$, and let C be a subgroup of $E^\times$ whose index $|E^\times : C|$ is a π-number. Then, for all fields $F \leq L \leq E$, the equality $L = \widehat{L \cap C}$ holds, except when the following conditions are mutually satisfied.*

(1) q is a Mersenne prime,
(2) e is even,
(3) $L = \mathbb{F}_{q^2}$, and
(4) 4 does not divide $|C|$.

When these simultaneously hold, $L \cap C = F \cap C$, so $\widehat{L \cap C} = F < L$.

3. **Character Degree Computations**

Our concluding section presents the computations for the character degree set of the split extension $C \rtimes \mathrm{Gal}(E/F)$. In the prior paper [4], this was accomplished only in the case where $\mathcal{E} = \mathcal{E}_0$. All standard notations and conventions regarding character theory are taken from [1]. The following generalizes Theorem 5 from [4], itself generalizing Theorem 3.2 in [3]. Our proof here supersedes and is a modification of that proof. In particular, this proof now includes the excepted Mersenne situation.

Proof of Theorem 1.1. Due to Itô's theorem (Theorem 6.15 of [1]), every degree in $\mathrm{cd}(G)$ divides $|G : C| = |\Gamma| = e$.

Consider a character $\mu \in \mathrm{Irr}(C)$. Let Ψ be the stabilizer of μ in Γ. It follows that $C\Psi$ is the stabilizer of μ in G. As $C\Gamma/C \cong \Gamma$ is cyclic, we see that μ extends to $\mathrm{Irr}(C\Psi)$ (Corollary 11.22 of [1]) and by Gallagher's theorem, every irreducible constituent of $\mu^{C\Psi}$ is an extension of μ. Applying the Clifford correspondence (Theorem 6.11 of [1]), we see that every irreducible constituent of $\mu^{C\Psi}$ induces irreducibly to G. We conclude that every irreducible constituent of μ^G has degree $|\Gamma : \Psi|$. Conversely, since every irreducible character of G lies over some character $\mu \in \mathrm{Irr}(C)$, every degree in $\mathrm{cd}(G)$ arises in this manner.

We now establish some notation to be used throughout the remainder of the proof. First, when we reference the "exceptional case," we specifically mean that (i)-(iii) hold (q is Mersenne, e is even, and 4 does not divide $|C|$). Let λ be a generator for the cyclic group $\mathrm{Irr}(C)$. Note that λ is a faithful character and a homomorphism from C to the complex numbers. Let c be a generator for the group C, and σ a generator for Γ. (In particular, we may take σ to be the Frobenius automorphism of E.)

Consider an arbitrary integer m and element $\tau \in \Gamma$. Because λ is a homomorphism, $\lambda^m(d) = \lambda(d^m)$ for all elements $d \in C$. We compute

$$(\lambda^m)^\tau(d) = \lambda^m(d^{\tau^{-1}}) = \lambda\big((d^{\tau^{-1}})^m\big) = \lambda\big((d^m)^{\tau^{-1}}\big).$$

Thus, $(\lambda^m)^\tau = \lambda^m$ if and only if $\lambda\big((d^m)^{\tau^{-1}}\big) = \lambda(d^m)$ for all $d \in C$. Since λ is faithful, this will occur if and only if $(d^m)^{\tau^{-1}} = d^m$ for all $d \in C$. It follows that τ stabilizes λ^m if and only if τ centralizes d^m for every element $d \in C$. The latter happens exactly when τ centralizes $\langle c^m \rangle$.

We next show, in the exceptional case, that 2 is not a degree of G. By the second paragraph, it suffices to show that $\langle \sigma^2 \rangle$ is not the stabilizer of any character in $\mathrm{Irr}(C)$. In other words, we need to prove that if σ^2 stabilizes λ^l for some integer l, then σ stabilizes λ^l. In the fourth paragraph, we have seen that σ^2 stabilizes λ^l if and only if σ^2 centralizes c^l. Let K be the fixed field for σ^2 in E. It follows that K is the extension field of F whose degree is 2. (I.e., $K = \mathbb{F}_{q^2}$.) From Theorem 2.5, we know that $K \cap C = F \cap C$. Now, we see that σ^2 stabilizes λ^l if and only if $c^l \in K \cap C = F \cap C$. But $c^l \in F$ implies that σ stabilizes λ^l, as needed.

Now, let n be an arbitrary divisor of e, and assume in the exceptional case that $n \neq 2$. Let $\Phi = \langle \sigma^n \rangle$, and observe that $|\Gamma : \Phi| = n$. Write L for the fixed field of σ^n in E. Note that $\Phi = \mathrm{Gal}(E/L)$, that σ^n fixes the subgroup $L \cap C$ of C, and that if $n \neq 2$, then $L = \mathbb{F}_{q^n} \neq \mathbb{F}_{q^2}$. Since c is a generator of C, there is some integer m for which $L \cap C = \langle c^m \rangle$.

We now compute the stabilizer of λ^m in Γ. Let $\tau \in \Gamma$ be arbitrary. By the fourth paragraph, τ stabilizes λ^m if and only if τ centralizes $\langle c^m \rangle = L \cap C$. This occurs if and only if τ centralizes $\widehat{L \cap C}$. Applying Theorem 2.5, we know that $L = \widehat{L \cap C}$. Thus, τ stabilizes λ^m if and only if $\tau \in \mathrm{Gal}(E/L) = \Phi$. We conclude that Φ is the stabilizer of λ^m, and applying the second paragraph, we have $n \in \mathrm{cd}(G)$. □

References

[1] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, San Diego, 1976.

[2] O. Manz and T. R. Wolf, *Representations of Solvable Groups*, Cambridge University Press, Cambridge, 1993.

[3] J. K. McVey, Prime divisibility among degrees of solvable groups, *Comm. Algebra*, **32** (2004) 3391–3402.

[4] J. K. McVey, On a Galois connection between the subfield lattice and the multiplicative subgroup lattice, *Pacific J. Math.* **264** (2013) 213-219.

[5] J. Riedl, Character degrees, class sizes, and normal subgroups of a certain class of p-groups." *J. Algebra* **218** (1999) 190–215.

[6] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. f. Math.* **3** (1892) 265–284.

Mark L. Lewis

Department of Mathematical Sciences, Kent State University, Kent, Ohio 44242, United States of America

Email: lewis@math.kent.edu

John K. McVey

Department of Mathematical Sciences, Kent State University, Kent, Ohio 44242, United States of America

Email: jmcvey@math.kent.edu