FIELD EQUIVALENT FINITE GROUPS

by

Alexander Moretó and Gabriel Navarro
Facultat de Matemàtiques
Universitat de València
Burjassot, València 46100
SPAIN

E-mail: alexander.moreto@uv.es, gabriel@uv.es

Research partially supported by the Ministerio de Ciencia y Tecnología, Grants BFM2001-1667-C03-02, BMF-2001-0180. The first author is also supported by the Programa Ramón y Cajal.

1. INTRODUCTION

M. Isaacs has given the following definition: two finite groups X and Y are **field equivalent** if there is a bijection $\chi \mapsto \chi'$ from $\mathrm{Irr}(X)$ onto $\mathrm{Irr}(Y)$ such that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi')$ for every $\chi \in \mathrm{Irr}(X)$, where $\mathrm{Irr}(X)$ is the set of complex irreducible characters of X and $\mathbb{Q}(\chi)$ is the field of values of χ. In this paper, we give solution to a problem proposed by him.

THEOREM A. *Suppose that G is field equivalent to a cyclic group. Then G is cyclic.*

In general, we cannot expect much more than this. For instance, there exists a group G of order 64 with 16 conjugacy classes such that all of its irreducible characters are rational valued. Hence, G is field equivalent to an elementary abelian 2-group and G is not abelian. Even more, there exists another group H of order 32 with 11 conjugacy classes and rational valued characters. In particular, H is field equivalent to the symmetric group of degree 6.

There is an application of Theorem A: if A acts coprimely on a finite group G, then the fields of values of the A-invariant irreducible characters of G determine if the fixed points subgroup $\mathbf{C}_G(A)$ is cyclic. (See Section 4 below.)

2. GROUPS OF ODD ORDER

We notice that a finite group G is field equivalent with a cyclic group C of order n if and only if

$$\mathrm{Irr}(G) = \bigcup_{d|n} \mathrm{Irr}_d(G)\,,$$

where $\mathrm{Irr}_d(G) \cap \mathrm{Irr}_e(G) = \emptyset$ if $d \neq e$, $|\mathrm{Irr}_d(G)| = \varphi(d)$, and if $\psi \in \mathrm{Irr}_d(G)$, then $\mathbb{Q}(\psi) = \mathbb{Q}_d$, the cyclotomic field of d-th roots of unity. This easily follows by writing $\mathrm{Irr}_d(C) = \{\lambda \in \mathrm{Irr}(C) \,|\, o(\lambda) = d\}$, and noticing that if $\lambda \in \mathrm{Irr}_d(C)$, then $\mathbb{Q}(\lambda) = \mathbb{Q}_d$. Since groups of odd order are exactly the groups with exactly one real character, we have that $|G|$ is odd if and only if n is odd.

In order to use inductive arguments in groups of odd order, it is convenient to have the following weaker hypothesis.

(2.1) HYPOTHESIS. *Suppose that G is a finite group such that*

$$\mathrm{Irr}(G) = \bigcup_{d\in A} \mathrm{Irr}_d(G)\,,$$

where A is a set of positive odd integers such that if $\psi \in \mathrm{Irr}_d(G)$, then $\mathbb{Q}(\psi) = \mathbb{Q}_d$ and $|\mathrm{Irr}_d(G)| = \varphi(d)$.

Our aim in this Section is to classify all finite groups satisfying Hypothesis (2.1).

Throughout this paper, we shall use an elementary fact on cyclotomic fields: if $d \leq e$ are positive integers, then $\mathbb{Q}_d \subseteq \mathbb{Q}_e$ if and only if d divides e or e is odd and $d = 2f$, for some f dividing e. Hence, if e and d are odd , then $\mathbb{Q}_d \subseteq \mathbb{Q}_e$ if and only if d divides e and therefore $\mathbb{Q}_d = \mathbb{Q}_e$ only if $d = e$. If a group G satisfies (2.1) and $d \in A$, then notice that

G has exactly $\varphi(d)$ characters χ with $\mathbb{Q}(\chi) = \mathbb{Q}_d$ and all of them are Galois conjugate. In particular, if a group G satisfies (2.1), then all factor groups of G satisfy (2.1). Notice too that groups satisfying (2.1) are of odd order. Finally, if $\chi \in \mathrm{Irr}(G)$ is such that $\mathbb{Q}(\chi) = \mathbb{Q}_f$, where f is odd, then $f \in A$.

(2.2) LEMMA. *Suppose that G is a nilpotent group satisfying (2.1). Then G is cyclic.*

Proof. Since $G/\Phi(G)$ satisfies (2.1), we may assume that the Sylow subgroups of G are elementary abelian. Now let p be a prime divisor of $|G|$ and let $\lambda \in \mathrm{Irr}(G)$ be of order p. Then $\mathbb{Q}(\lambda) = \mathbb{Q}_p$ and G has exactly $p-1$ irreducible characters with field of values $\mathbb{Q}_p$. Hence all Sylow subgroups of G are cyclic. ∎

We shall repeatedly use the following fact.

(2.3) LEMMA. *Suppose that G has a normal Sylow p-subgroup P and let $\theta \in \mathrm{Irr}(P)$. If T is the stabilizer of θ in G and $\hat{\theta}$ is the canonical extension of θ to T, then $\chi = \hat{\theta}^G \in \mathrm{Irr}(G)$ lies over θ and $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\theta)$.*

Proof. By Corollary (8.16) of [3], there exists a unique $\hat{\theta} \in \mathrm{Irr}(T)$ extending θ such that the determinantal order of $\hat{\theta}$ is a power of p. In fact $o(\theta) = o(\hat{\theta})$. (This is called the *canonical extension* of θ to T.) Now, χ lies over θ and $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\hat{\theta})$. Since θ uniquely determines $\hat{\theta}$, it follows that $\mathbb{Q}(\theta) = \mathbb{Q}(\hat{\theta})$. ∎

(2.4) THEOREM. *Suppose that G is a group satisfying (2.1). Suppose that G has an elementary normal p-subgroup V such that G/V has a normal p-complement and a cyclic Sylow p-subgroup. If $\lambda \in \mathrm{Irr}(V)$ has order p, then $\{\lambda, \lambda^2, \dots, \lambda^{p-1}\}$ is a complete set of representatives of G-orbits on $\mathrm{Irr}(V) - 1_V$.*

Proof. We may write $G/V = (K/V)(P/V)$, where $K/V \lhd G/V$ has p'-order, $P \in \mathrm{Syl}_p(G)$ and P/V is cyclic. Suppose that $|P/V| = p^f$. Since P/V is isomorphic to a quotient of G, we have that for $e \leq f$, G has exactly $\varphi(p^e)$ irreducible characters with field of values $\mathbb{Q}_{p^e}$, all having K in its kernel.

Let $1 \neq \lambda \in \mathrm{Irr}(V)$ and let $T = I_G(\lambda)$ be the stabilizer of λ in G. Now, by Corollary (8.16) of [3], there exists a unique $\hat{\lambda} \in \mathrm{Irr}(T \cap K)$ of order p extending λ. Also, by uniqueness, we have that $\hat{\lambda}$ is T-invariant. In particular, if $L = \ker(\hat{\lambda})$, then $L \lhd T$. Also, $|(T \cap K)/L| = p$. Now, $T/T \cap K$ is cyclic, and therefore $\hat{\lambda}$ extends to T. Suppose that the cyclic group $T/T \cap K$ has order p^d. We have that $d \leq f$. If $\beta \in \mathrm{Irr}(T)$ lies over $\hat{\lambda}$, we have that β extends $\hat{\lambda}$ and $\beta^{p^{d+1}} = 1$. We have that $\mathbb{Q}(\beta^G) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}_{p^{d+1}}$. Since $\mathbb{Q}(\beta^G) = \mathbb{Q}_{p^e}$ for some $e \leq d+1$ and K is not contained in the kernel of β^G, necessarily $e > f$. Then $e = f+1$, $d = f$, $\mathbb{Q}(\beta^G) = \mathbb{Q}_{p^{f+1}}$ and $\mathbb{Q}(\beta) = \mathbb{Q}_{p^{f+1}}$. In particular, $o(\beta) = p^{f+1}$. Since $L \subseteq \ker(\beta)$, we deduce that T/L is cyclic of order p^{f+1}. Now, by considering the p^f extensions β of $\hat{\lambda}$ to T, we notice that G has p^f different irreducible characters with field of values $\mathbb{Q}_{p^{f+1}}$ lying over λ.

Suppose now that $\lambda^g = \lambda^s$ for some $g \in G$ and $1 < s < p$. Then $T^g = I_G(\lambda^s) = T$. Hence, $g \in \mathbf{N}_G(T)$. By the uniqueness of canonical extensions, we easily have that $\hat{\lambda}^g = \hat{\lambda}^s$ and also $\ker(\hat{\lambda}) = \ker(\hat{\lambda}^s) = \ker(\hat{\lambda}^g) = L^g$. Thus g also normalizes L. Write $T/L = \langle yL \rangle$ and notice that $y^{g^{-1}}L = y^n L$ for some $1 \leq n$ coprime with p. Now, let $\beta \in \mathrm{Irr}(T)$ be over $\hat{\lambda}$ and let $\chi = \beta^G \in \mathrm{Irr}(G)$, which we know has field of values $\mathbb{Q}_{p^{f+1}}$. Now, we have that $\beta^g = \beta^n$. Hence, $\hat{\lambda}^g = \hat{\lambda}^n = \hat{\lambda}^s$ and therefore $n \equiv s \bmod p$. Now, let σ be the Galois automorphism of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ fixing p'-roots of unity and sending each p-power order root of unity ξ to ξ^n. Then

$$\chi^\sigma = (\beta^\sigma)^G = (\beta^n)^G = (\beta^g)^G = \beta^G = \chi\,,$$

and therefore σ fixes $\mathbb{Q}_{p^{f+1}} = \mathbb{Q}(\chi)$. Then σ fixes $\mathbb{Q}_p$ and therefore $n \equiv 1 \bmod p$. Thus $s \equiv 1 \bmod p$, and this is impossible.

Hence, for each $1 \leq j \leq p-1$, we have at least p^f irreducible characters of G with field of values $\mathbb{Q}_{p^{f+1}}$ lying over λ^j. This gives rise to at least $p^f(p-1) = \varphi(p^{f+1})$ irreducible characters, and we conclude that there are no more. This implies the theorem. ∎

In what follows, we shall use a well-known fact: if V is a faithful irreducible $GF(p)C$-module, where C is cyclic of order m, then $|V| = p^n$, where n is the order of p modulo m.

(2.5) LEMMA. *Suppose that V is a faithful irreducible $GF(p)C$-module of dimension n, where C is cyclic of order e coprime with p. Suppose that there exists $v \in V$ such that $\{v, 2v, \ldots, (p-1)v\}$ is a complete set of representatives of C-orbits on $V - \{0\}$. Then $|C| = p^n - 1/p - 1$ and $(p-1, e) = 1$.*

Proof. Our hypotheses easily imply that $\mathbf{C}_C(v) = \mathbf{C}_C(V) = 1$ and therefore $\mathbf{C}_C(w) = 1$ for all $0 \neq w \in V$. Hence, $|C| = p^n - 1/p - 1 = e$. Let $d = (p-1, e)$ and let D be the subgroup of C of order d. Now, let W be a simple D-submodule of V. Then W is faithful and if $|W| = p^m$, we know that m is the order of p modulo d. Hence $m = 1$. If $1 \neq x \in D$ and $0 \neq w \in W$, we have that $wx = kw$ for some $1 < k < p$. Now, $w = jvc$ for some $c \in C$ and $1 \leq j < p$, and we conclude that $vx = kv$. This is not possible. ∎

In the proof of the following result, we use a nontrivial theorem of E. Shult, namely, if A acts as automorphisms on an odd p-group P transitively permuting the subgroups of order p of P, then P is abelian ([6]).

(2.6) THEOREM. *Suppose that G is a group satifying (2.1) with Fitting length 2. Let N be the smallest normal subgroup of G such that G/N is nilpotent. Then $G = NC$, where C is cyclic, $(|N|, |C|) = 1$ and N is nilpotent such that all of its Sylow subgroups are non-cyclic elementary abelian and minimal normal subgroups of G.*

Proof. By Lemma (2.2), we have that G/N is cyclic. Also, by hypothesis, $1 < N$ is nilpotent.

First, we want to see that $(|G/N|, |N|) = 1$. Let p be a common prime divisor of $|N|$ and $|G/N|$. If K is the p-complement of N, by working in G/K (which has Fitting length two) we may assume that N is a p-group. Since G/N is abelian, we have that G has a normal Sylow p-subgroup $P > N$. We may write $G = PD$, where D is a cyclic p'-group, $[P, D] \subseteq N$ and P/N is cyclic. Since p divides $|G/N|$, we have that G/N has a linear irreducible character of order p. Hence, all the $p-1$ irreducible characters ψ of G with $\mathbb{Q}(\psi) = \mathbb{Q}_p$ contain N in the kernel. Suppose that P is not cyclic. Then $P/\Phi(P)$ is not cyclic and therefore there exists $\lambda \in \mathrm{Irr}(P)$ linear of order p with N not contained in its kernel. By Lemma (2.3), there exists $\chi \in \mathrm{Irr}(G)$ lying over λ with $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_p$. Now, $\mathbb{Q}(\chi) = \mathbb{Q}_f$ for some odd integer f, and we deduce that $\mathbb{Q}(\chi) = \mathbb{Q}_p$. This is impossible. Therefore, P is cyclic. Since $P = [P, D] \times \mathbf{C}_P(D)$, we conclude that $[P, D] = 1$. Hence, G is abelian, and this is a contradiction. We conclude that $(|G/N|, |N|) = 1$.

We may write $G = NC$, where C is cyclic and $(|N|, |C|) = 1$. It remains to show that the Sylow subgroups of N are non-cyclic elementary abelian minimal normal subgroups of G. Let $P \in \mathrm{Syl}_p(N)$ and notice that PC is isomorphic to a factor group of G with Fitting length two. Hence, it is no loss if we assume that $N = P$. Also, since $G/\mathbf{C}_C(P)$ cannot be nilpotent, we may assume that $\mathbf{C}_C(P) = \mathbf{C}_C(P/\Phi(P)) = 1$.

By Theorem (2.4), if $1 \neq \lambda \in \mathrm{Irr}(P/\Phi(P))$, we know that $\{\lambda, \lambda^2, \ldots, \lambda^{p-1}\}$ is a complete set of representatives of C-orbits on $\mathrm{Irr}(P/\Phi(P)) - 1_P$. Since C is abelian, notice that all nontrivial irreducible characters of $P/\Phi(P)$ have the same stabilizer T. Now, the elements of $T \cap C$ fix every irreducible character in $P/\Phi(P)$ and we deduce that $T \cap C = \mathbf{C}_C(P/\Phi(P)) = 1$ and $T = P$. In particular, we have that $\mathrm{Irr}(P/\Phi(P))$ is an irreducible faithful C-module. Thus, if $|P/\Phi(P)| = p^n$, by Lemma (2.5), we have that $|C| = p^n - 1/p - 1 = e$ with $(e, p-1) = 1$. If $P/\Phi(P) = \langle\lambda\rangle$ is cyclic, then $n = 1$ and $[C, P] = 1$. Hence G is nilpotent and this is not possible. Hence, P is not cyclic.

Notice now that G exactly has $p - 1$ irreducible characters with field of values $\mathbb{Q}_p$, and these are lying over $\lambda, \lambda^2, \ldots, \lambda^{p-1}$, respectively, where $1 \neq \lambda \in \mathrm{Irr}(P/\Phi(P))$.

Suppose that P/P' is not elementary abelian. Hence $P' < \Phi(P)$ and let $U/P' = \Phi(\Phi(P)/P')$. Now, $U \triangleleft G$, P/U is abelian and $\exp(P/U) = p^2$. Now, $\Phi(P)/U \subseteq \Omega_1(P/U) \triangleleft G/U$. Hence, $\Phi(P)/U = \Omega_1(P/U)$. In particular, P/U is a direct product of n cyclic groups of order p^2.

Suppose that $\mu \in \mathrm{Irr}(P/U)$ is one of the $p^{2n} - p^n$ characters of P/U of order p^2. By Lemma (2.3), there exists $\chi \in \mathrm{Irr}(G)$ over μ with $\mathbb{Q}(\chi) = \mathbb{Q}_a \subseteq \mathbb{Q}_{p^2}$ for some odd integer a. Now, a divides p^2 and necessarily $a = p^2$. Hence there are exactly $\varphi(p^2) = p(p-1)$ irreducible characters in G with field of values $\mathbb{Q}_{p^2}$. This implies that the $p^{2n} - p^n$ characters of order p^2 lie in at most $p(p-1)$ different C-orbits. On the other hand, if $x \in C$ fixes μ, then x fixes μ^p and thus $x \in P$. Hence, each C-orbit exactly contains $\frac{p^n-1}{p-1}$ elements. Then

$$p^{2n} - p^n \leq p(p-1)\frac{p^n - 1}{p - 1}$$

and $n = 1$, which is not possible.

We wish to prove that P is abelian. We may assume that P' is a minimal normal subgroup of G, and therefore elementary abelian. Also, $P' \subseteq \mathbf{Z}(P)$. Since P/P' is a chief factor of G, we have that $Z = \mathbf{Z}(P) = P'$. Now, the exponent of P divides p^2. Hence, if $\theta \in \mathrm{Irr}(P)$, $\mathbb{Q}(\theta) \subseteq \mathbb{Q}_{p^2}$. If $\theta \in \mathrm{Irr}(P)$ does not contain P' in its kernel, by Lemma (2.3), there exists $\chi \in \mathrm{Irr}(G)$ lying over θ such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\theta) \subseteq \mathbb{Q}_{p^2}$. Since the irreducible characters of G with field of values $\mathbb{Q}_p$ contain P' in its kernel, we deduce that $\mathbb{Q}(\chi) = \mathbb{Q}(\theta) = \mathbb{Q}_{p^2}$. In particular, the exponent of P is p^2. Now, since P/Z is abelian, Z is elementary abelian and p is odd, we have that

$$\Omega_1(P) = \langle x \in P | x^p = 1\rangle = \{x \in P | x^p = 1\} < P\,.$$

We conclude that all the subgroups of order p of P lie inside Z. By coprime action, and using that p is odd, it is well-known that $\mathbf{C}_C(Z) = \mathbf{C}_C(P) = 1$. Hence Z is a faithful irreducible C-module and therefore $|Z| = |P/P'| = p^n$. Now, we claim that C acts transitively on the subgroups of order p of Z. Let $1 \neq z \in Z$ and suppose that $c \in C$ fixes $\langle z \rangle$. Then $z^c = z^k$ for some $1 \leq k < p$. Since $(e, p-1) = 1$, we deduce that $z^c = z$. Then c centralizes $\langle z^u | u \in C \rangle = Z$, and this is impossible. Therefore the stabilizer of $\langle z \rangle$ in C is trivial. Since there are $p^n - 1/p - 1 = |C|$ subgroups of order p in Z, we conclude that C acts transitively on them. By Shult's theorem, this is a contradiction.

Finally, since P is an irreducible C-module, we have that P is a minimal normal subgroup of G. ∎

In the next result, we use a well-known theorem of Brodkey ([1]): if a finite group G has an abelian Sylow p-subgroup P, then there is $g \in G$ such that $P \cap P^g = \mathbf{O}_p(G)$.

(2.7) THEOREM. *If G satisfies (2.1), then the Fitting length of G is at most 2.*

Proof. We argue by induction on $|G|$. We may assume that G has a minimal normal subgroup V such that the Fitting length of G is 3 and G/V has Fitting length 2. We have that V is an elementary abelian p-group.

By Theorem (2.6), we know the structure of G/V. We have that $G/V = (N/V)(C/V)$, where N/V and C/V are coprime, C/V is cyclic and the Sylow subgroups of N/V are non-cyclic elementary abelian. Also, N is not nilpotent.

First, we prove that p does not divide $|N/V|$. Suppose it does. By taking a linear character of N/V of order p and using Lemma (2.3), we see that there are exactly $p-1$ irreducible characters of G with field of values $\mathbb{Q}_p$ all of them having V in their kernel. Let Q/V be a Sylow p-subgroup of G/V, which is normal in G/V. Also Q/V is elementary abelian and $\Phi(Q) \subseteq V$. Hence, the exponent of Q is at most p^2 and all irreducible characters of Q have their values in $\mathbb{Q}_{p^2}$. Let $\mu \in \mathrm{Irr}(Q)$ be not containing V in its kernel. By Lemma (2.3), there exists $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\mu) \subseteq \mathbb{Q}_{p^2}$. Necessarily, $\mathbb{Q}(\chi) = \mathbb{Q}(\mu) = \mathbb{Q}_{p^2}$. In particular, $V = \Phi(Q)$. Now, we have that a p-complement H of N acts trivially on $Q/\Phi(Q)$. Thus $[H, Q] = 1$. So N is nilpotent and this is impossible.

Now, by Theorem (2.4), we have that the stabilizers of all nontrivial elements of $\mathrm{Irr}(V)$ are G-conjugate.

Now, $\mathbf{C}_N(V) = U \times V$, where $U \lhd G$ and $U \subseteq \mathbf{Z}(N)$. If $U > 1$, by induction we have that N/U is nilpotent, and therefore N is nilpotent. So we may assume that $\mathbf{C}_N(V) = V$.

Let q be a prime dividing $|N : V|$ and let $X/V \in \mathrm{Syl}_q(N/V)$. Hence, X/V is a normal abelian Sylow q-subgroup of G/V. Let $S \in \mathrm{Syl}_q(X)$. By Brodkey's theorem, there exists $v \in V$ such that $S \cap S^v = 1$. Therefore $\mathbf{C}_S(v) = 1$. Since the actions of S on V and on $\mathrm{Irr}(V)$ are permutation isomorphic (by Theorem (13.24) of [3]), there exists $\lambda \in \mathrm{Irr}(V)$ such that $T \cap X = V$, where T is the stabilizer of λ in G. Now, $T \cap X/V$ is a Sylow q-subgroup of T/V and we deduce that T/V is a q'-group. Now, if $\mu \in \mathrm{Irr}(V)$ and I is its stabilizer in G, we deduce that I/V is a q'-group. In particular, $I \cap X = V$. Then $\mu^X \in \mathrm{Irr}(X)$ for all $1 \neq \mu \in \mathrm{Irr}(V)$ and we deduce that $\mathbf{C}_S(w) = 1$ for all $1 \neq w \in V$. Then X is a Frobenius group and S is a Frobenius complement of odd order. Hence, S is cyclic, and this is impossible. ∎

3. PROOF OF THEOREM A

In the proof of our main result, we use the following result of Iwasaki ([4]). For the reader's convenience, we write down a proof.

(3.1) LEMMA. *If G has at most two real valued characters, then a Sylow 2-subgroup of G is normal.*

Proof. We argue by induction on $|G|$, and we may assume that G is of even order. We have that G has exactly two real classes. Hence, the only nontrivial real class K is the class of involutions of G. If x, y are involutions, then xy is real, and therefore xy is an involution. Thus $N = K \cup 1$ is a normal 2-subgroup of G. If G/N has exactly one real character, then G/N is of odd order, and we are done. Otherwise, we apply induction. ∎

We will also use the following result of Amit and Chillag.

(3.2) THEOREM. *Suppose that G is a solvable group and let $\chi \in \mathrm{Irr}(G)$ with $\mathbb{Q}(\chi) = \mathbb{Q}_f$. Then G has an element of order f.*

Proof. See Theorem (22.1) of [5]. ∎

(3.3) LEMMA. *Suppose that $F = GF(2^m)$ and let $\sigma \in \mathrm{Gal}(F)$ be of order $q > 1$ odd. Let Γ be the semidirect product of $K = F^\times$ with $I = \langle \sigma \rangle$. Suppose that $H \leq \Gamma$ is not cyclic and has order divisible by $2^m - 1$. Then there exists $\psi \in \mathrm{Irr}(H)$ such that $\mathbb{Q}(\psi)$ is not a cyclotomic field.*

Proof. We claim that there exists $P \in \mathrm{Syl}_p(K)$ such that I acts Frobenius on P. Suppose that $m \neq 6$. Let p be a Zsigmondy prime for $2^m - 1$. (See, for instance, Theorem (6.2) of [5].) If $1 \neq \tau \in I$ has order $d|m$, then $|\mathbf{C}_K(\tau)| = 2^{m/d} - 1$ which is not divisible by p. If $P \in \mathrm{Syl}_p(K)$, we have that $\mathbf{C}_P(\tau) = 1$. Thus I acts Frobenius on P. If $m = 6$, then $q = 3$ and in this case we can take P of order 7.

Now, since P is cyclic, we have that $q|p-1$ and P is a normal Sylow p-subgroup of Γ. Hence, $P \subseteq H$, by hypothesis. Now, let $\lambda \in \mathrm{Irr}(P)$ be of order p. Notice that $I_\Gamma(\lambda) = K$ because $I_I(\lambda) = 1$. Hence, $K \cap H$ is the stabilizer of λ in H. Let $\nu \in \mathrm{Irr}(K \cap H)$ be the canonical extension of λ to $K \cap H$, so that $o(\nu) = p$. If $h \in H$ fixes ν, then h fixes λ and therefore $h \in K \cap H$. Hence, by the Clifford correspondence, we have that $\psi = \nu^H \in \mathrm{Irr}(H)$. Since H is not cyclic, we have that $K \cap H < H$. Now, if $h \in H - (K \cap H)$, we have that $\nu^h = \nu^r$ for some integer r with $1 < r < p$. Now, $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. We claim that $\mathbb{Q}(\psi)$ cannot be $\mathbb{Q}_p$. If σ is the Galois automorphism fixing p'-roots of unity and sending p-power roots of unity ξ to ξ^r, then

$$\psi^\sigma = (\nu^r)^H = (\nu^h)^H = \nu^H = \psi \,,$$

and this proves the claim. ∎

(3.4) THEOREM. *Suppose that G is field equivalent with a cyclic group of order n. Then G is cyclic.*

Proof. By hypothesis, we have that

$$\mathrm{Irr}(G) = \bigcup_{d|n} \mathrm{Irr}_d(G)\,,$$

where $\mathrm{Irr}_d(G) \cap \mathrm{Irr}_e(G) = \emptyset$ if $d \neq e$, $|\mathrm{Irr}_d(G)| = \varphi(d)$, and if $\psi \in \mathrm{Irr}_d(G)$, then $\mathbb{Q}(\psi) = \mathbb{Q}_d$. We notice that G has at most two real valued characters. By Lemma (3.1), we have that $P \triangleleft G$, where $P \in \mathrm{Syl}_2(G)$. Let H be a 2-complement of G.

Suppose that G has odd order. Then n is odd and G satisfies (2.1). If G is nilpotent, then G is cyclic and we are done. By Theorems (2.6) and (2.7), we may assume that $G = NC$, where C is cyclic and $1 < N$ is abelian with $(|N|, |C|) = 1$. Also, the Sylow subgroups of N are not cyclic and minimal normal subgroups of G. Let p be any prime divisor of $|N|$. Now, G has an irreducible character with field of values $\mathbb{Q}_{|C|}$. Hence, $|C|$ divides n. Also, by Lemma (2.3), G has an irreducible character with field of values $\mathbb{Q}_p$, where p divides n. Thus $p|C|$ divides n, and G has irreducible characters with field of values $\mathbb{Q}_{p|C|}$. By Theorem (3.2), G has an element x of order $p|C|$. Write $x = uv$, where $u \in N$ has order p, v has order $|C|$ and $uv = vu$. Then $o(vN) = o(v) = |G/N|$, and we deduce that $N\langle v\rangle = G$. Then $u \in \mathbf{Z}(G)$ and $\langle u\rangle$ is a normal subgroup of G. Then $\langle u\rangle$ is a Sylow p-subgroup of N, and this is not possible.

So we may assume that G is of even order. Hence, n is even and G has a unique real valued non-trivial character χ. Let $\delta \in \mathrm{Irr}(P)$ of order 2. By Lemma (2.3), δ lies under χ, and we deduce that H transitively permutes the nontrivial elements of $\mathrm{Irr}(P/\Phi(P))$. Write $|P/\Phi(P)| = 2^v$. If T is the stabilizer of δ in H, then $\mathbf{C}_H(P) \subseteq T$ and $|H : T| = 2^v - 1$.

Write $n = 2^e m$, where m is odd. We claim that

$$\mathrm{Irr}(G/\Phi(P)) = \bigcup_{d|2m} \mathrm{Irr}_d(G)\,.$$

Suppose that $\psi \in \mathrm{Irr}(G)$ has $\Phi(P)$ in its kernel and suppose that $\mathbb{Q}(\psi) = \mathbb{Q}_f$ for some $f|n$. Now, since the exponent of $G/\Phi(P)$ has 2-part 2, we have that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_{|G|_{2'}}$ and therefore f_2 divides 2. Hence, f divides $2m$. Conversely, suppose that $\psi \in \mathrm{Irr}_d(G)$, where $d|2m$. Then $\mathbb{Q}(\psi) = \mathbb{Q}_f$ for some odd number f. Let $\mu \in \mathrm{Irr}(P)$ be under ψ. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{|G|_{2'}})$ (which necessarily has 2-power order). Then σ fixes ψ and therefore $\mu^\sigma = \mu^x$ for some $x \in G/P$. Since $o(x)$ is odd, we conclude that $\mu^\sigma = \mu$. Hence, μ has rational values. By Lemma (2.3), we conclude that μ lies under some rational valued character, which necessarily is χ. Then μ is G-conjugate to δ, and the claim follows.

If $\Phi(P) > 1$, arguing by induction, we have that $G/\Phi(P)$ is cyclic. Therefore $P/\Phi(P)$ and H are cyclic. Hence P is cyclic, $G = P \times H$, and therefore G is cyclic. Thus, we may assume that $\Phi(P) = 1$. Therefore, $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_{|G|_{2'}}$ for all $\psi \in \mathrm{Irr}(G)$. In particular, we have that $n_2 = 2$, since otherwise there would exist $\psi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\psi) = \mathbb{Q}_4 = \mathbb{Q}(i)$, and this is not possible.

Suppose that P is cyclic. Then $|P| = 2$ and $G = P \times H$. Then $n = |\mathrm{Irr}(G)| = 2|\mathrm{Irr}(H)|$, where $|\mathrm{Irr}(H)| = m$ is odd. Now, for each d dividing m, there exist exactly $2\varphi(d)$ irreducible characters of G with field of valued $\mathbb{Q}_d$. If $\chi \in \mathrm{Irr}(G)$, we have that $\chi = 1 \times \alpha$ or $\chi = \delta \times \alpha$, for some $\alpha \in \mathrm{Irr}(H)$ and in both cases $\mathbb{Q}(\chi) = \mathbb{Q}(\alpha)$. This easily implies that there are exactly $\varphi(d)$ irreducible characters of H with field of values $\mathbb{Q}_d$. Hence, H is field equivalent to the cyclic group of m elements, and H is cyclic, by the second paragraph of this proof. Thus G is cyclic in this case. Hence, we may assume that $v \geq 2$.

By Theorem (6.8) of [5], we deduce that $H/\mathbf{C}_H(P)$ is a subgroup of Γ, where Γ is as in Lemma (3.3). Now, $H/\mathbf{C}_H(P)$ is isomorphic to a quotient of G, and therefore all of its irreducible characters have cyclotomic fields of values. By Lemma (3.3), we deduce that $H/\mathbf{C}_H(P)$ is cyclic. In particular, $T \triangleleft H$ and we easily have that $T = \mathbf{C}_H(P)$.

Notice that the stabilizer of δ in G is $I = P\mathbf{C}_H(P)$. If $\psi \in \mathrm{Irr}(G)$ does not contain P in its kernel, then ψ lies over δ and therefore $\psi = (\hat{\delta}\alpha)^G$, where $\hat{\delta} \in \mathrm{Irr}(I)$ is the canonical extension of δ to I and $\alpha \in \mathrm{Irr}(\mathbf{C}_H(P))$. Hence, by using the Clifford correspondence and Corollary (6.17) of [3], we have that

$$|\mathrm{Irr}(G)| = |\mathrm{Irr}(H)| + |\mathrm{Irr}(\mathbf{C}_H(P))|\,.$$

Since H is of odd order, by a theorem of Burnside (Problem (3.17) of [3]), we have that

$$|\mathrm{Irr}(G)| \equiv |H| + |\mathbf{C}_H(P)| = |\mathbf{C}_H(P)|(|H/\mathbf{C}_H(P)| + 1) = 2^v|\mathbf{C}_H(P)| \bmod 16\,.$$

Hence, we deduce that 4 divides $|\mathrm{Irr}(G)| = n$, and this was not possible. ∎

4. COPRIME ACTION

If X and Y are finite groups and $A \subseteq \mathrm{Irr}(X)$ and $B \subseteq \mathrm{Irr}(Y)$, we say that A and B are **field equivalent** if there exists a bijection $\chi \mapsto \chi'$ from A onto B such that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi')$ for all $\chi \in A$.

(4.1) THEOREM. *Suppose that A acts coprimely on G and let $C = \mathbf{C}_G(A)$. Then C is cyclic if and only $\mathrm{Irr}_A(G)$ is field equivalent with the set of irreducible characters of a cyclic group.*

Proof. It is well-known that the Glauberman-Isaacs correspondence $^* : \mathrm{Irr}_A(G) \to \mathrm{Irr}(C)$ preserves fields of values. (See Chapter 13 of [3] and Section 10 of [2].) Now, Theorem A applies. ∎

REFERENCES

[1] J. S. Brodkey, A note on finite groups with an abelian Sylow group. Proc. Amer. Math. Soc. **14** (1963), 132–133.

[2] M. Isaacs, Characters of solvable and symplectic groups, Amer. J. Math. **95** (1973), 594–635.

[3] M. Isaacs, Character Theory of Finite Groups, Dover, New York, 1994.

[4] S. Iwasaki, On finite groups with exactly two real conjugate classes. Arch. Math. (Basel) **33** (1979/80), no. 6, 512–517.

[5] O. Manz, T. Wolf, Representations of Solvable Groups, Camdridge University Press, 1993.

[6] E. Shult, On finite automorphic algebras. Illinois J. Math. **13** (1969), 625–653.