Proceedings of the Edinburgh Mathematical Society (1988) 31, 469–474 ©

ON THE DETERMINATION OF THE RAMIFICATION INDEX IN CLIFFORD'S THEOREM

by ROBERT W. VAN DER WAALL

(Received 6th February 1987)

(Dedicated to Professor Dr B. Huppert on his sixtieth birthday)

Introduction

Let K be a field, G a finite group, V a (right) KG-module. If H is a subgroup of G, then, restricting the action of G on V to H, V is also a KH-module. Notation: V_H.

Suppose N is a normal subgroup of G. The KN-module V_N is not irreducible in general, even when V is irreducible as KG-module. A part of the well-known theorem of A. H. Clifford [**1**, V.17.3] yields the following.

Theorem (A. H. Clifford). *Let V be an irreducible KG-module. Let $N \trianglelefteq G$. Then V is a completely reducible KN-module. Moreover*

$$V_N = V_1 \dotplus \cdots \dotplus V_n,$$

where $V_i \not\simeq V_j$ as KN-modules if $i \neq j$, and each V_i is a direct sum of e isomorphic copies of an irreducible KN-submodule W_i, say, and $W_i \not\simeq W_j$ if $i \neq j$. We write $V_i = eW_i$. It holds that

$$V_N \simeq e(W_1 \dotplus \cdots \dotplus W_n) = \underbrace{W_1 \dotplus \cdots \dotplus W_1}_{e \text{ times}} \dotplus \cdots \dotplus \underbrace{W_n \dotplus \cdots \dotplus W_n}_{e \text{ times}}.$$

There exists a group A with $N \subseteq A \subseteq G$, $|G:A| = n$, and a KA-submodule T of V such that $T_N = eW_1$ and $V \simeq T \bigotimes_{KA} KG$, as KG-modules. The integer e is called the inertia index (or ramification index) of V over N. It is independent of $i \in \{1, \ldots, n\}$.

Consider the groups G, A, N as in Clifford's Theorem. It is important to know what the actual value of e is, in particular whether e divides the order of A/N. In two well-known cases it is indeed true that e divides $|A/N|$, namely

1. K algebraically closed of characteristic zero or of positive characteristic not dividing the order of G (see [**6**, p. 35]).
2. K a finite field of odd characteristic not dividing the order of G and containing the primitive mth-roots of unity, where $m = |G|_{2'}$, G/N an elementary abelian p-group (see [**4**, Theorem 13]), due to W. Willems.

It is not true that the divisibility property of the inertia index always holds. As an example, take R cyclic of order 3, $K=\mathbb{F}_2$, $\{1\}=N \lhd R$. Then there exists an irreducible two-dimensional $\mathbb{F}_2$-representation of R with inertia index 2 over N. So here $e \nmid |R/N|$.

In [5, Theorem E], it was shown that $e=1$, $e=q$ or $e|q-1$ in the case where G/N has prime order q, G arbitrary finite, K any finite field. It is the purpose of this paper to generalize that Theorem E of [5], and to give full information about the number e in the case where G/N is cyclic of prime power order and K is a finite field. It follows from Clifford's Theorem that it is sufficient to consider the homogeneous case $V_N=eW$, W an irreducible KN-submodule of the irreducible KG-module V. As a corollary to our results we conclude that e always divides $|G/N|$ in the case where G/N is a cyclic 2-group and K is a finite field.

Most of the notation is standard and can be found in [1, 2, 3] or is otherwise clear or self-explanatory. We use:

$\bar{E}$ = an algebraic closure of the field E,
$\mathbb{F}_t$ = finite field consisting of t elements,
$\mathbb{F}(\chi)$: see the definition given in the last lines of page 151 of [3].

This paper is dedicated to Professor Dr B. Huppert on the occasion of his sixtieth birthday, as a token of homage to him for all his work in finite group theory. Needless to say the books he has written will be landmarks for ever.

The theorems and their proofs

Theorem 1. *Let G be a finite group, $N \trianglelefteq G$, G/N cyclic of order q^n, q prime. Assume V is an irreducible $\mathbb{F}G$-module for a certain finite field $\mathbb{F}$. Suppose V_N is a direct sum of e irreducible $\mathbb{F}N$-submodules, each isomorphic to the irreducible $\mathbb{F}N$-submodule U of V_N. We write $V_N=eU$. Let $\mathbb{F}(\eta)=\mathbb{F}(\eta(n)|n\in N)$, where η is the trace function of some irreducible constituent of the $\bar{\mathbb{F}}N$-module $U \otimes_{\mathbb{F}} \bar{\mathbb{F}}$. Put $X \supseteq N$, $|G/X|=q$. Suppose V_X is homogeneous but not irreducible. Then $e \geqq 2$ and either* (1) *or* (2) *holds.*

1. *Suppose $e=q^a$, $a\geqq 1$. Then* $(\operatorname{char}\mathbb{F}, q)=1$ *and $q\,\|\,|\mathbb{F}(\eta)|-1$. There exists an irreducible $\mathbb{F}M$-submodule W of V such that $N \trianglelefteq M \trianglelefteq G$, $|G/M|=q^a$, $V_M=q^aW$, $W_M=U$, unless $q=2$ and $|\mathbb{F}(\eta)|\equiv -1 \pmod 4$. If $q=2$ and $2^\beta\,\|\,|\mathbb{F}(\eta)|+1$, $2^{\beta+1}\nmid|\mathbb{F}(\eta)|+1$, $\beta\geqq 2$, then there exists an irreducible $\mathbb{F}M$-submodule W of V with $N \trianglelefteq M \trianglelefteq G$, $|G/M|=2^{a+\beta-1}$, $V_M=2^aW$, $W_N=U$, unless $e=2$.*
2. *Suppose e does not divide $|G/N|$. Then* $(\operatorname{char}\mathbb{F}, q)=1$. *It holds that e divides $\phi(|G/N|)=q^{n-1}(q-1)$. So q is odd. Write $e=fq^{\gamma-1}$, $f|q-1$. Then $2\leqq f$ and f is the order of $|\mathbb{F}(\eta)|$ modulo q. When $\gamma\geqq 2$, then there exists an irreducible $\mathbb{F}M$-submodule W of V with $N \trianglelefteq M \trianglelefteq G$, $|G/M|=q^a$, $V_M=eW$, $W_N=U$, where $q^a\,\|\,|\mathbb{F}(\eta)|^e-1$ but $q^{a+1}\nmid|F(\eta)|^e-1$.*

It follows from the construction of the proof of Theorem 1, that each of the cases actually occurs in practice.

The following observation elucidates why the case $e=2$ deserves separate treatment.

Remark 2. Let K be a finite field such that $2^\beta\,\|\,|K|+1$, $2^{\beta+1}\nmid|K|+1$, $\beta\geqq 2$. Let G be a cyclic group of order $2^n \geqq 4$. Then G admits a two-dimensional irreducible K-representation. Its restriction to $N=\{1\}$ is twice the trivial K-representation of $\{1\}$.

Proof of Theorem 1. It turns out that $q \neq \operatorname{char} \mathbb{F}$ for otherwise Green's Theorem VII.9.19 of [**2**] yields $e=1$. By Theorem VII.2.6 of [**2**] there exists a finite field K containing $\mathbb{F}$ such that K is a splitting field for G and all its sections. Consider $V \otimes_{\mathbb{F}} K$. Then, for suitable integers u and s, we have the following decompositions into irreducible KG-modules R_j and irreducible KN-modules T_j:

$$V \underset{\mathbb{F}}{\otimes} K = R_1 \dot{+} \cdots \dot{+} R_u, \quad (eU) \underset{\mathbb{F}}{\otimes} K \cong e\left(U \underset{\mathbb{F}}{\otimes} K\right) = e(T_1 \dot{+} \cdots \dot{+} T_s).$$

By [**2**, VII.1.16(e)] it follows that the R_i are pairwise non-isomorphic absolutely irreducible KG-modules affording characters which are galois conjugated to each other; see also [**4**, 9.21]. The same statement holds for the KN-modules T_i.

(1) *Let $R_{1|N}$ be not homogeneous.* Let W be an irreducible constituent of the KN-module $R_{1|N}$. By considering the algebraic closure of K, the fact that G/N is cyclic, Clifford's Theorem, the fact that $\operatorname{char} K \nmid |G/N|$, and combining these with Theorems 9.9. and 9.18 of Chapter VII of [**2**], it follows that $R_{1|N}$ is a direct sum of pairwise non-isomorphic KN-submodules of $R_{1|N}$. Such a W is isomorphic to some T_i, as KN-modules. It follows that, say, $R_{1|N} \cong T_1 \dot{+} \cdots \dot{+} T_f$. The inertia group I of T_1 in G is here different from G by assumption. Hence $X \supseteq I \supseteq N$ as G/N is cyclic of prime power order. The ramification index of R_1 over X is one (by [**2**, VII.9.18]) and $f=|G/I| \geqq 2$. Therefore there exists an irreducible KI-module D with $D \otimes_{KI} KG \cong R_1$. Hence $D \otimes_{KI} KX$ is an irreducible constituent of $R_{1|X}$. So $R_{1|X}$ decomposes into a direct sum of q pairwise non-isomorphic irreducible KX-modules, again by [**2**, VII.9.18]. Each of these modules gives R_1 when induced up to G. By galois conjugacy something similar holds for each of the $R_1, \ldots, R_u$. It follows that $(V \otimes_{\mathbb{F}} K)_X$ is a direct sum of pairwise non-isomorphic irreducible KN-modules. However this is in conflict with the assumption that V_X should be homogeneous but not irreducible.

(2) *Suppose now that all $R_{i|N}$ are homogeneous.* Then, by [2, VII. 9.9] and [**2**, VII. 9.18] combined with the facts G/N cyclic, Clifford's Theorem, $\operatorname{char} K \nmid |G/N|$, it now follows that all the $R_{i|N}$ are absolutely irreducible KN-modules. Let now χ be the trace function of R_i. Note that the field $\mathbb{F}(\chi)$ does not depend on the index i, by [**4**, 9.21(c)]. So we have $V \otimes_{\mathbb{F}} \mathbb{F}(\chi) = S_1 \dot{+} \cdots \dot{+} S_u$, where, say, $R_i \cong S_i \otimes_{\mathbb{F}(\chi)} K$, and where $S_i \not\cong S_j$ if $i \neq j$, as $\mathbb{F}(\chi)G$-modules. Observe that any S_i is an absolutely irreducible $\mathbb{F}(\chi)G$-module. Since $R_{i|N}$ is an absolutely irreducible KN-module, it holds that $S_{i|N}$ is an absolutely irreducible $\mathbb{F}(\chi)N$-module, for any i. Notice that $u=[\mathbb{F}(\chi):\mathbb{F}]=|\operatorname{Gal}(\mathbb{F}(\chi)/\mathbb{F})|$ and that $\operatorname{Gal}(\mathbb{F}(\chi)/\mathbb{F})$ is cyclic, generated by the Frobenius automorphism $x \mapsto x^{|\mathbb{F}|}$, any $x \in \mathbb{F}(\chi)$. We have $et=u$, where t is determined by $(V \otimes_{\mathbb{F}} \mathbb{F}(\chi))_N = (S_1 \dot{+} \cdots \dot{+} S_u)_N \cong e(U \otimes_{\mathbb{F}} \mathbb{F}(\chi)) = e(L_1 \dot{+} \cdots \dot{+} L_t)$; the L_i are pairwise non-isomorphic (absolutely) irreducible $\mathbb{F}(\chi)N$-submodules of $U \otimes_{\mathbb{F}} \mathbb{F}(\chi)$. Consider $\mathbb{F}(\eta)$, where η is the trace function of an irreducible $\bar{K}N$-submodule of $U \otimes_{\mathbb{F}} \bar{K}$. Hence $\mathbb{F}(\eta) \subseteq K$. Then $t=s$, where $U \otimes_{\mathbb{F}} \mathbb{F}(\eta) = Y_1 \dot{+} \cdots \dot{+} Y_s$ is the decomposition into (absolutely) irreducible $\mathbb{F}(\eta)$-submodules of $U \otimes_{\mathbb{F}} \mathbb{F}(\eta)$. Since $\operatorname{Gal}(K/\mathbb{F})$ is cyclic, it is easily seen that $\mathbb{F}(\eta) \subseteq \mathbb{F}(\chi)$.

(2.1) *Assume from now on that* $e \geqq 2$. Then some of the $S_{i|N}$ are isomorphic to one and the same (absolutely) irreducible $\mathbb{F}(\chi)N$-submodule A of $U \otimes_{\mathbb{F}} \mathbb{F}(\chi)$. Let the cardinality of the set S, consisting of all these S_i with $S_{i|N} \cong A$, be c. Without loss of generality, put $S = \{S_1, S_2, \ldots, S_c\}$. Then, just as it is done in [5, Theorem E, Proof], it follows that $cs = u = ct$ and that $c = |\mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F}_r)|$, where $r = |\mathbb{F}|^s$. Hence $c = e$. Let $\langle \gamma \rangle = \mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F}_r)$. Then, according to [2, VII.9.13], a unique one-dimensional $\mathbb{F}(\chi)G$-module Λ exists, on which N acts trivially, such that $S_1^\gamma \cong S_1 \otimes_{\mathbb{F}(\chi)} \Lambda$. By iteration and employing [2, VII.9.12(c)], it follows that Λ^h is equal to the trivial one-dimensional $\mathbb{F}(\chi)G$-module, where $h = (r^e - 1)/(r-1)$. The order of Λ divides $|G/N|$. So $|\Lambda| = q^a$, $a \leqq n$. Since $1 \neq \gamma$, $a \geqq 1$ holds. Further, it follows from a repeated application of γ that no integer $(r^i - 1)/(r-1)$ is a multiple of q^a for any $i = 1, \ldots, e-1$. We now consider two possibilities: (1) $q \mid r-1$, (2) $q \nmid r-1$.

(2.1.1) *Let* $q \mid r-1$. Suppose $q^m \mid r-1$ but $q^{m+1} \nmid r-1$. In the cases $\{q \text{ odd}, m \geqq 1\}$ and $\{q = 2, m \geqq 2\}$ it follows that the integer $(r^{q^k g} - 1)/(r-1)$ with $q \nmid g$ and $k \geqq 0$, has precisely k divisors q in its prime decomposition. From this it follows that $e = q^a$. On the other hand, in the case $\{q = 2, m = 1\}$ we can write $r = 2^\beta v - 1$ with $\beta \geqq 2$, $2 \nmid v$. It follows that for $k \geqq 1$, $2 \nmid g$, the integer $(r^{2^k g} - 1)/(r-1)$ has precisely $\beta + k - 1$ divisors 2 in its prime decomposition. Observe that for $k = 0$ $(r^g - 1)/(r-1)$ is odd.

Suppose for the moment that $m \neq 1$. Then order $\Lambda = q^a = e$ ($q = 2$ is possible here). Let $N \subseteq M \subseteq G$, $M \trianglelefteq G$, $|G/M| = q^a$. Then Λ_M is the trivial one-dimensional $\mathbb{F}(\chi)M$-module. Hence $S_{1|M} \cong S_{2|M} \cong \cdots \cong S_{e|M}$, and $S_{1|M}$ is an irreducible $\mathbb{F}(\chi)M$-module. Since $S_{1|N}$ is an absolutely irreducible $\mathbb{F}(\chi)N$-module, we see that $S_{1|M}$ is even absolutely irreducible as an $\mathbb{F}(\chi)M$-module. Consider $V_M = d(X_1 \dotplus \cdots \dotplus X_z)$, $d \geqq 1$, the X_i's irreducible $\mathbb{F}M$-submodules of V, $X_i \ncong X_j$ if $i \neq j$, as $\mathbb{F}M$-modules. Using $S_{1|M} \cong S_{i|M}$ for each $i = 1, \ldots, e$, it follows from the Deuring–Noether Theorem applied on the irreducible constituents of $V_M \otimes_{\mathbb{F}} \mathbb{F}(\chi)$, that $e \leqq d$. However, regarding $eU = V_N$ via $V_{M|N}$, $d \leqq e$ holds. Hence $d = e$, $z = 1$ and so $V_M = eX_1 = q^a X_1$, $X_{1|N} \cong U$.

Now let $m = 1$, $q = 2$, $r = 2^\beta v - 1$, $\beta \geqq 2$, $2 \nmid v$. We see that if $e = 2^\delta$ with $\delta \geqq 2$, then order $\Lambda = 2^{\beta + \delta - 1}$. Conversely, when order $\Lambda = 2^{\beta + w}$, $w \geqq 1$, then $e = 2^{w+1}$. Just as before it now follows that there exists an irreducible $\mathbb{F}M$-submodule W of V with $N \trianglelefteq M \trianglelefteq G$, $|G/M| = 2^{\beta + \delta - 1}$, $V_M = 2^\delta W$, $W_N = U$. The case $e = 2$ is treated in Remark 2.

(2.1.2) *Let* $q \nmid r-1$. Since also $q \nmid r = |\mathbb{F}|^s$, it follows that q is odd. Then obviously e is equal to the order of r modulo q^a. Hence $e \mid q^{a-1}(q-1)$, by Euler's Theorem. Hence, as $q^a \| |G/N|$, we have $e \mid \phi(|G/N|) = q^{n-1}(q-1)$. So write $e = q^{\gamma - 1} f$, $1 \leqq \gamma \leqq a$, $f \mid q-1$. Observe $f \geqq 2$. For otherwise, just by $(r-1, q) = 1 = (r, q)$, we get a contradiction. Now suppose that $\gamma \geqq 2$ and that $q^\varepsilon \mid r^{fq^{\gamma-1}} - 1$, $\varepsilon > a$, $q^{\varepsilon+1} \nmid r^{fq^{\gamma-1}} - 1$. Then $q^{\varepsilon - 1} \mid r^{fq^{\gamma-2}} - 1$, whence $q^a \mid r^{fq^{\gamma-2}} - 1$, contrary to the definition of e. Hence we conclude that $q^a \mid r^e - 1$, $q^{a+1} \nmid r^e - 1$ if $\gamma \geqq 2$. Let $\hat{f}$ be the order of r modulo q. Hence $\hat{f} \mid f$. Also $q^a \mid r^{\hat{f} q^{a-1}} - 1$, whence $e \mid \hat{f} q^{a-1}$ by definition of e. Since $(q, f) = 1$, $fq^{\gamma-1} \mid \hat{f} q^{a-1}$ implies $f \mid \hat{f}$. Therefore $\hat{f} = f$. Again by the same reasoning as in (2.1.1) the required result on the $\mathbb{F}M$-module W now follows. Next suppose $\gamma = 1$. Here $e = f$ is the order of r modulo q^a. When $a \geqq 2$, then order $\hat{f}$ of r modulo q^{a-1} divides f. Also $q^a \mid r^{\hat{f} q} - 1$ and so $f \mid \hat{f} q$. Hence $f \mid \hat{f}$, whence $f = \hat{f}$. Inductively it follows that f is the order of r modulo q.

The proof of Theorem 1 is complete. □

https://doi.org/10.1017/S0013091500037664 Published online by Cambridge University Press

Proof of Remark 2. Let $m=\min\{n,\beta+1\}$. Suppose ζ is a primitive 2^m-th root of unity in some extension field of K. Hence ζ can be regarded as an element from $\mathbb{F}_{|K|^2}\supseteq K$, but here $\zeta\notin K$. It follows that the Frobenius automorphism $x\to x^{|K|}$ $(x\in\mathbb{F}_{|K|^2})$ of $\mathbb{F}_{|K|^2}$ has order 2 and $\zeta^{|K|}\neq\zeta$. By Exercise (9.6) of [4] there exists now an irreducible (possibly non-faithful) 2-dimensional K-representation of G. □

We come now to the final Theorem 3 in which the decomposing behaviour of V_N is demonstrated via normal subgroups between G and N.

Theorem 3. *Let G/N be cyclic of order q^n, q prime. Assume V is an irreducible $\mathbb{F}G$-module for a finite field $\mathbb{F}$. Suppose $V_N=eU$, U an irreducible $\mathbb{F}N$-submodule of V_N. Then precisely one of the following holds.*

(1) *If $N\trianglelefteq M\trianglelefteq G$, $|G/M|=q$, then V_M is the direct sum of q pairwise non-isomorphic irreducible $\mathbb{F}M$-submodules.*

(2) *There exists $N\trianglelefteq T\trianglelefteq G$ such that V_T is an irreducible $\mathbb{F}T$-module and either $e=1$ or Theorem 1 holds for $\{T, V_T, N, U\}$.*

In either case e divides $q^n(q-1)$ and $e\leqq q^n$.

Proof. We may assume that (1) does not hold and that $e\geqq 2$. Hence Theorem 1 holds for $\{G, V, N, U\}$ or, setting $N\trianglelefteq M\trianglelefteq G$ with $|G/M|=q$, V_M is irreducible as an $\mathbb{F}M$-module. So we assume that V_M is an irreducible $\mathbb{F}M$-module. Take any subgroup S of M with $N\subseteq S\subseteq M$. Note that $N\neq M$ by $e\geqq 2$. If V_S is not homogeneous, then the property G/S cyclic of prime power order would yield that V_M would not be homogeneous, a contradiction. Hence V_S is homogeneous. So there exists $N\subseteq L\subseteq T\subseteq M\subseteq G$ such that V_T is an irreducible $\mathbb{F}T$-module and such that V_L is homogeneous but not irreducible as an $\mathbb{F}L$-module, where $|T/L|=q$. Therefore Theorem 1 holds for $\{T, V_T, N, U\}$.

In case (1) we put $V_M=L_1\dotplus\cdots\dotplus L_q$ as the required sum decomposition. Hence $L_{i|N}=eq^{-1}U$ for each i, by the Krull–Schmidt Theorem. So by induction $e\,|\,q^n(q-1)$ and $e\leqq q^n$.

If in case (2) $T\neq G$ then by induction $e\,|\,|T/N|(q-1)$ and $e\leqq|T/N|$. Hence $e\,|\,q^n(q-1)$ and $e\leqq q^n$.

If in case (2) $T=G$ then we read of directly from Theorem 1 that $e\,|\,q^n(q-1)$ and $e\leqq q^n$. □

REFERENCES

1. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin–Heidelberg–New York, 1967).

2. B. Huppert and N. Blackburn, *Finite Groups II* (Springer-Verlag, Berlin–Heidelberg–New York, 1982).

3. I. M. Isaacs, *Character Theory of Finite Groups* (Academic Press, New York–London, 1976).

4. R. W. van der Waall, Minimal non-M-groups, *Indag. Math.* **42** (1980), 93–106.

5. R. W. van der Waall, On Clifford's theorem and ramification indices for symplectic modules over a finite field, *Proc. Edinburgh Math. Soc.* **30** (1987), 153–167.

6. W. Willems, *Induzierte und eingeschränkte Moduln über Gruppenringen* (Diplomarbeit, Mainz, 1973).

Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
The Netherlands

https://doi.org/10.1017/S0013091500037664 Published online by Cambridge University Press