J. Austral. Math. Soc. (Series A) 50 (1991), 297–315

KRONECKER CLASSES OF FIELD EXTENSIONS OF SMALL DEGREE

CHERYL E. PRAEGER

(Received 10 August 1989)

Communicated by H. Lausch

Abstract

The structure of Kronecker class of an extension $K : k$ of algebraic number fields of degree $|K : k| \leq 8$ is investigated. For such classes it is shown that the width and socle number are equal and are at most 2, and for those of width 2 the Galois group is given. Further, if $|K : k|$ is 3 or 4, or if $5 \leq |K : k| \leq 8$ and $K : k$ is Galois, then the groups corresponding to all "second minimal" fields in $\mathscr{K}$ are determined.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 20 B 25, 12 F 10.

1. Introduction

The study of Kronecker classes of algebraic number fields has led to several questions about covering properties of subgroups of a finite group. We examine these and obtain information about the structure of a Kronecker class over k which contains a field K such that the extension $K : k$ has small degree.

For an algebraic number field k and a finite extension K of k the *Kronecker set* $D(K|k)$ of K over k is defined as the set of all prime ideals of the ring of integers of k having a prime divisor of relative degree 1 in K. Following Jehne [3], we define two finite extensions of k to be *Kronecker equivalent* relative to k if their Kronecker sets over k have finite symmetric difference. The equivalence classes of this relation are called *Kronecker classes*. In [3, §2] it is shown that all the minimal fields in a Kronecker class

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

$\mathscr{K}$ relative to k have the same Galois hull (normal closure) M say over k; the field M is called the *Galois hull* $M(\mathscr{K})$ *of* $\mathscr{K}$ and the Galois group $G(\mathscr{K})$ of $M : k$ is called the *Galois group of* $\mathscr{K}$. Thus there are a finite number of minimal fields in $\mathscr{K}$ and the number of $G(\mathscr{K})$-classes of minimal fields in $\mathscr{K}$ is called the *width of* $\mathscr{K}$ and denoted $\omega_k(\mathscr{K})$. The set $\mathscr{M}(\mathscr{K})$ of intermediate subfields of $M(\mathscr{K}) : k$ which lie in $\mathscr{K}$ can be considered as a graph with respect to inclusion; this is called the *socle graph* of $\mathscr{K}$ and the number of $G(\mathscr{K})$-classes in $\mathscr{M}(\mathscr{K})$ is called the *socle number of* $\mathscr{K}$ and is denoted $\mu_k(\mathscr{K})$. For example, if a Kronecker class $\mathscr{K}$ over k contains a minimal field K such that $K : k$ is Galois, then $M(\mathscr{K}) = K$ and $\mu_k(\mathscr{K}) = \omega_k(\mathscr{K}) = 1$. In fact the socle graph consists of just a single vertex. In the first part of this paper we consider Kronecker classes $\mathscr{K}$ containing a minimal field K such that the degree of $K : k$ is at most 8 and show that $\mu_k(\mathscr{K}) = \omega_k(\mathscr{K}) \leq 2$; in the case of width 2 Kronecker classes $\mathscr{K}$, the group $G(\mathscr{K})$ and the conjugacy classes of the fixed groups of the two classes of minimal fields of $\mathscr{K}$ are determined.

THEOREM 1. *Suppose that a Kronecker class* $\mathscr{K}$ *relative to* k *contains a field* K *such that the extension* $K : k$ *has degree* $n \leq 8$. *Then* $\mu_k(\mathscr{K}) = \omega_k(\mathscr{K})$ *is* 1 *or* 2. *In the case where* $\mathscr{K}$ *has width* 2 *one of the following holds, where* U *and* V *are the fixed groups of* K *and of a representative* L *of the second class of minimal fields in* $\mathscr{K}$ *respectively.*

(a) $n = 5$, $G(\mathscr{K}) = A_5$, $U \simeq A_4$, $V \simeq S_3$, *so* $|L : k| = 10$.

(b) $n = 7$, $G(\mathscr{K}) = \mathrm{PSL}(2, 7)$, $U \simeq V \simeq S_4$, U *and* V *are not conjugate in* $G(\mathscr{K})$, *and* $|L : k| = 7$.

(c) $n = 8$, $|L : k| = 8$, *and one of the following holds*:

(i) $G(\mathscr{K}) = \mathrm{GL}(2, 3)$, $U \simeq V \simeq S_3$, *and* U *and* V *are not conjugate in* $G(\mathscr{K})$;

(ii) $G(\mathscr{K})$ *is the holomorph of a cyclic group of order* 8, U *and* V *are both elementary abelian of order* 4 *but are not conjugate in* $G(\mathscr{K})$;

(iii) $G(\mathscr{K}) = \mathbb{Z}_2 \operatorname{wr} C = \mathbb{Z}_2^4 \cdot C$ *where* $C = \mathbb{Z}_4$ *or* $\mathbb{Z}_2 \times \mathbb{Z}_2$, $U \simeq V \simeq \mathbb{Z}_2^3$ *with both* U *and* V *contained in the base group of the wreath product, but with* U *and* V *not conjugate in* $G(\mathscr{K})$.

The Kronecker equivalence of two extensions L and K of k is equivalent to a group theoretic condition; namely if $M : k$ is a Galois extension containing L and K as intermediate fields and if G is the Galois group of $M : k$ and U, V are the fixed groups of K and L respectively, then it is shown in [3, §1] that K and L are Kronecker equivalent over k if and only if $U^G = V^G$ where, for a subgroup H of G, H^G denotes the set theoretic union $\bigcup_{g \in G} H^g$. This group theoretic condition is studied in Section 2;

the group theoretic analogue, Theorem 2, of Theorem 1, is proved there and Theorem 1 is deduced from it. A similar result to Theorem 2 was obtained independently by N. Klingen in [7, Theorem 3.2]. In his paper the result is exploited to yield information about a variety of decomposition laws for number fields, where Kronecker equivalence corresponds to possessing the same weak decomposition law. In this paper the result is used to explore further the structure of Kronecker classes containing small degree extensions. A field L in a Kronecker class $\mathscr{K}$ over k is called a *second minimal field* in $\mathscr{K}$ if $k < L' < L$ for some $L' \in \mathscr{K}$ and L is minimal with respect to this property. For Kronecker classes containing a Galois extension $K : k$ of degree at most 8, the second minimal fields are completely determined: namely for each second minimal field L the Galois group of the Galois hull $\tilde{L} : k$ of L is determined together with the fixed groups of L and K. This was done in [9, 10] for $K : k$ of degree 4 or 8. There are no second minimal fields when $|K : k| = 2$ by [12], and the degrees 3, 5, 6 and 7 are dealt with in Theorem 3.3. The case of non-Galois extensions is considerably more complicated computationally. Section 3 contains a discussion of the general problem, and then determines the Galois group of the Galois hull $\tilde{L} : k$ of each second minimal L in $\mathscr{K}$ in the cases $n = 3, 4$. The results for $n = 3$ and $n = 4$ may be summarised as follows.

THEOREM 3. *Suppose that a Kronecker class $\mathscr{K}$ relative to k contains a field K such that the extension $K : k$ has degree $n = 3$ or $n = 4$. Then the only minimal fields in $\mathscr{K}$ are conjugates of K, and either $\mathscr{K}$ consists entirely of the algebraic conjugates of K, or $\mathscr{K}$ contains exactly one class of second minimal fields and there is a field L in this class containing K; further L and the Galois group $\tilde{G}$ of the Galois hull $\tilde{L}$ of $L : k$ is such that one of the following holds.*

(a) *$n = 3$, $K : k$ is Galois, $|L : K| = 2$, and $\tilde{G}$ is A_4.*

(b) *$n = 4$, $K : k$ is Galois, $|L : K| = 3$, and $\tilde{G}$ is a Frobenius group of order 72.*

(c) *$n = 4$, $K : k$ is not a Galois extension, $|L : K| = 3$, and $\tilde{G}$ is a semidirect product $S \cdot Q$, where S is elementary abelian of order 9 and Q is a semidihedral group of order 16.*

This theorem follows immediately from [9, Theorem 4.3], Theorem 3.3, and Lemmas 3.5 to 3.7. It has the following immediate corollary about Kronecker classes.

COROLLARY. *Let $\mathscr{K}$ be a Kronecker class relative to k containing a non-Galois extension K of k. If either $|K : k| = 3$, or $|K : k| = 4$ and the*

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

Galois group of $\mathscr{K}$ is A_4 or S_4, then $\mathscr{K}$ consists entirely of the algebraic conjugates of K; that is, the decomposition law of K over k is absolutely rigid in the sense of Klingen [7].

Note that in these situations K was known to be "rigid" over k by [6], and this result establishes the stronger property of absolute rigidity.

Moreover if $\mathscr{K}$ contains an extension $K : k$ of degree n and has Galois group A_n with $n > 5$, or S_n, then Guralnick [2] showed that K is absolutely rigid over k. Theorems 1 and 3 show that K is not absolutely rigid in the cases where n is 3 or 5 and the Galois group is A_n. Thus we have a complete solution to the problem of absolute rigidity in the case of alternating or symmetric Galois groups.

2. Covering properties of subgroups of small index

Suppose as in Theorem 1, that a Kronecker class $\mathscr{K}$ over k contains a minimal field K with $|K : k| = n \leq 8$. If $K : k$ is Galois then $\mathscr{K}$ has width and socle number 1 so assume that $K : k$ is not Galois and let M be the normal closure of $K : k$, that is, $M = M(\mathscr{K})$ is the Galois hull of $\mathscr{K}$. Then if $A = G(\mathscr{K})$ is the Galois group of $M : k$ and U is the fixed group of K, the A-core of U, $U_A = \bigcap_{a \in A} U^a$, is trivial and hence A acts faithfully and transitively by right multiplication as a permutation group on the set $\Omega = [A : U]$ of n right cosets of U in A. If $L \in \mathscr{K}$ and $L \leq M$ then the fixed group V of L in A is such that $U^A = V^A$. We determine all possibilities for V in the following Theorem 2.

THEOREM 2. *Suppose that A is a transitive permutation group of degree $n \leq 8$ and that the stabilizer U of a point is nontrivial. Suppose also that V is a subgroup of A such that $U^A = V^A$. Let $t = |A : V|$. Then one of the following holds.*

(a) *U and V are conjugate in A, so $t = n$.*

(b) $n = 5$, $t = 10$, $A = A_5$, $U = A_4$, $V = (S_2 \times S_3) \cap A_5 \simeq S_3$.

(c) $n = 6$, $t = 3$, $A \simeq A_4$, $U = Z_2$, $U < V = \mathbb{Z}_2 \times \mathbb{Z}_2 < A$.

(d) $n = t = 7$, $A = \mathrm{PSL}(2, 7)$ *and* $U \simeq V \simeq S_4$ *with U and V in different conjugacy classes.*

(e) $n = t = 8$ *and one of the following holds*:

(i) $A = \mathrm{GL}(2, 3)$, $U \simeq V \simeq S_3$, *and V has orbits of lengths* $2, 3, 3$;

(ii) *A is a holomorph of a cyclic group of order* 8, $U \simeq V$ *are elementary abelian of order* 4, *and V has orbits of lengths* $2, 2, 4$;

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

(iii) $A = \mathbb{Z}_2 \operatorname{wr} \mathbb{Z}_4$ *preserving the partition* $\{12|34|56|78\}$, *and* $U = \langle (34), (56), (78)\rangle$ *and* $V = \langle (12), (34)(56), (34)(78)\rangle$ *are both elementary abelian of order* 8;

(iv) $A = \mathbb{Z}_2 \operatorname{wr} \ (\mathbb{Z}_2 \times \mathbb{Z}_2)$ *preserving the partition* $\{12|34|56|78\}$ *with* U *and* V *as in* (iii).

It is easy to deduce Theorem 1 from Theorem 2. Clearly $\mu_k(\mathscr{K}) = \omega_k(\mathscr{K}) = 1$ unless one of (b) to (e) of Theorem 2 holds. In case (c) the group U does not correspond to a minimal field in $\mathscr{K}$. In cases (b), (d) and (e) there are $\mu_k(\mathscr{K}) = \omega_k(\mathscr{K}) = 2$ classes of intermediate fields of $M : k$ in $\mathscr{K}$ and Theorem 1 follows. This result was obtained independently by Klingen [7, Theorem 3.2] (see also [4, 5, 6]). The proof in [7] makes use of a computer verification of certain properties whereas the proof given here does not require a computer.

Proof of Theorem 2. The set $U^A = V^A$ is a union of conjugacy classes of A. Since U contains a conjugate of a non-identity element of V we may replace V by one of its conjugates if necessary and assume that $U \cap V \neq \{1\}$ and that $|U \cap V|$ is maximal among the intersection sizes $|U \cap V^a|$, for $a \in A$. If G is A_n or S_n then, by [6], $G = A_5$ and (b) is true, so we may assume that G is not A_n or S_n. Then since $U \neq \{1\}$ we must have $n \geq 4$. If $n = 4$, then A is D_8, and as $U^A = V^A$, we obtain $U = V$. If $n = 5$ then A is D_{10} or a Frobenius group F of order 20, and as $U^A = V^A$, $U = V$. Assume now that $n = 6$. If A is primitive of degree 6 then A is $\mathrm{PGL}(2, 5)$ or $\mathrm{PSL}(2, 5)$ [13] and so U and hence V contains an element of order 5. If V fixes a point then $V \leq U$ and in each case $V = U$. If V does not fix a point then V is transitive, and as 5 divides $|V|$, V is 2-transitive of degree 6 and hence $V \geq \mathrm{PSL}(2, 5)$. This means however that V contains an element of type 3^2 which contradicts the fact that $V^A = U^A$. Thus we may assume that A is imprimitive of degree 6. Assume first that $A \leq S_3 \operatorname{wr} S_2$. Then $U \leq S_2 \times S_3$ and so neither U nor V contains elements of type 3^2. In particular V is intransitive and does not have two orbits of length 3. If U and hence V contains an element of order 3 then V has an orbit of length 3 and V fixes a point; thus $V \leq U$ and as $U^A = V^A$ we obtain $V = U$. If 3 does not divide $|U|$ then, as U is nontrivial, $A = D_{12}$ and $U = V \simeq Z_2$. Thus we may assume that $A \leq S_2 \operatorname{wr} S_3 = B \cdot S_3$, the group of permutations preserving the partition $\{12|34|56\}$, and that $U \leq D_8$, the stabilizer of the point 1. The stabilizer D_8 of 1 contains permutations of types 1^6, 2^1, 2^2 (two classes), and 4^1 only. If V fixes a point then $V \leq U$ and it is easily checked that $V = U$. (Recall that there are two classes in $S_2 \operatorname{wr} S_3$ of permutations of

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

type 2^2.) Assume then that V has no fixed points. Suppose that V contains an element g of type 4^1, say $g = (3456)$. Then V has orbits $\{1, 2\}$ and $\{3, 4, 5, 6\}$. Now V must contain an element $(12)h$ and hence also $(12)hg$ for some $h \in \langle(3456), (35)\rangle$, and as V contains no elements of types 2^3 or $2^1 4^1$ we obtain a contradiction. Thus V contains no element of type 4^1 and hence U and V are elementary abelian. Suppose now that V contains an element g of type 2^1, say $g = (12)$. Now V contains an element h that moves the point 5 and not both of h and gh can have type 2^1. Hence V contains an element h of type 2^2 moving the point 5. Since V contains no elements of type 2^3 and since h centralizes g we must have $h = (12)(56)$ so that V contains (56). Similarly V contains (34) and hence V contains $(12)(34)(56)$ which is a contradiction. Thus U and V contain elements of types 1^6 and 2^2 only. As V fixes no points, $|V| \geq 4$. If V has an orbit of length 4 it must act regularly on it and hence there are elements of type 2^1 or 2^3 in V which is not allowed. Thus V has three orbits of length 2 and $|V| = 4$. It follows that $V = A \cap B = B \cap A_6$, $A = V \cdot \mathbb{Z}_3 \simeq A_4$ and $\mathbb{Z}_2 \simeq U < V$.

If $n = 7$ then A is PSL(2, 7), or is a Frobenius group of order dividing 42 (see [13]). In the latter case $V = U$ since $V^A = U^A$. If $A = \mathrm{PSL}(2, 7)$ then $U \simeq S_4$ contains permutations of types 2^2, 3^2 and $2^1 4^1$, and it follows that the V-orbits have lengths 1, 6 or 3, 4. In the former case $V \leq U$ and as V contains elements of orders 3 and 4, $V = U$. In the latter case also $V \simeq S_4$ and is not conjugate to U. Thus we may assume that $n = 8$. If A is PSL(2, 7) or PGL(2, 7) then U is a Frobenius group of order 21 or 42 respectively and we must have $V = U$. If A is primitive with a regular normal subgroup N then by [13], 7 divides $|U|$ and $|V|$. In this case if V is transitive then either V contains N or $A = \mathrm{AGL}(3, 2) > V = \mathrm{PSL}(2, 7)$ by [11], and so V contains a fixed point free element, contradicting $U^A = V^A$. Thus V fixes a point and so $V \leq U$ and it follows that $V = U$. So we may assume that A is imprimitive.

Suppose first that a minimal block of imprimivity for A has size 4. Then $A \leq S_4 \operatorname{wr} S_2$ and 3 divides $|A|$. It follows that U and V contain an element of type 3^2. If V fixes a point then $V \leq U \leq S_3 \times S_4$ and it follows that $V = U$. So suppose that V does not fix a point. Since V contains an element of type 3^2 and V contains no fixed point free element, V has two orbits of length 4, namely the blocks of imprimitivity for A. If the stabilizer of a point in V fixes more than one point an easy counting argument shows that V contains an element with no fixed points. Hence the stabilizer in V of a point in one block is still transitive on the other block, so V contains O_2 $(S_4 \operatorname{wr} S_2)$ which contains a fixed point free element, a contradiction.

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

Finally assume that A has blocks of size 2 so that $A \leq S_2 \operatorname{wr} S_4 = B \cdot S_4$, the group of permutations preserving the partition $\{12|34|56|78\}$. We may assume that U is the stabilizer of the point 1. Suppose first that $U \cap B = \{1\}$. Then $U \lesssim S_3$. If U had order 2 or 3 then U and V would be equal so we may assume that $U \simeq S_3$ and hence that A is $\mathbb{Z}_2 \times S_4$ or $\mathrm{GL}(2, 3)$. In the former case elements of order 2 in U are of type 2^2 and it follows that $V = U$ fixes a point, or $V \simeq S_3$ has orbits of lengths 2, 3, 3, and case (e)(i) holds. Next suppose that $U \cap B$ has order 2. Then $A \cap B$ has order 4 and it follows that $U \cap B$ fixes four points, say $1, 2, 3$ and 4. Thus A preserves the partition $\{1234|5678\}$ and hence $|U| \leq 4$. Suppose that $U \neq V$. Then U is elementary abelian of order 4 and hence $A/(A \cap B) \simeq D_8$ and we may assume that $U \cap V = U \cap B = \langle a = (56)(78)\rangle$ and that V has no fixed point. Then $A \cap B = \langle a, b = (12)(34)\rangle$. Suppose first that A contains an element of order 8. Then without loss of generality A contains $c = (15372648)$. Also A contains an element d such that d inverts c modulo $A \cap B$, and (by multiplying by ab if necessary) we may assume that $d \in U$ fixes 1, 2 and fixes $\{3, 4\}$ setwise. It follows that d is either $d' = (34)(57)(68)$ or $d'' = (34)(58)(67) = ad'$ (from the fact that U is not cyclic), and $U = \{1, a, d', d''\}$. Now V contains a conjugate of each of d' and d'', and up to conjugacy in A, $V = \{1, a, d'^c = (14)(23)(78), ad'^c = (14)(23)(56) = (d'')^{c^3}\}$. Thus (e)(ii) holds. Now suppose that A has an element c of order 4 cyclically permuting the B-orbits: we may take $c = (1537)(2648)$. Also U contains an element d which inverts c modulo $A \cap B$, and as U is not cyclic, d is either $d' = (57)(68)$ or $d'' = d'a = (58)(67)$. Then $U = \{1, a, d', d''\}$. Now V must contain conjugates of d' and d'' which do not fix 1, and there is only one possibility for these elements, namely $d'^c = (13)(24)$ and $d''^c = (14)(32)$. However $\langle a, d'^c, d''^c\rangle$ contains an element with no fixed points, which is a contradiction to the fact that $U^A = V^A$.

Now suppose that $|U \cap B| = 4$. It follows that $A \cap B = B \cap A_8$ and so $V \cap B$ consists of permutations of types 1^8 and 2^2 only. It then follows that $V \cap B$ fixes a point. If 3 divides $|A|$ then $V = U$. If $A = (A \cap B) \cdot D_8$ or $A = (A \cap B) \cdot Z_4$ then there are two conjugacy classes of involutions of type 2^2 in $A \cap B$ and therefore U, and hence V, contain members of both classes; it follows that $V = U$. If $A = (A \cap B) \cdot (\mathbb{Z}_2 \times \mathbb{Z}_2)$ there are three conjugacy classes of involutions of type 2^2 in $A \cap B$ and again U and V contain members of each class so $V = U$. Assume now that $|U \cap B| = 8$, that is, $B \subseteq A$. Then, as $V \cap B$ must contain permutations of types $2^1, 2^2, 2^3$ but none of type 2^4, we may assume that $V \cap B$ is one of $U \cap B$, $V_2 = \langle (34), (56)(78)\rangle$, $V_3 = \langle (12), (34)(56), (34)(78)\rangle$. If 3 divides $|A|$ then U contains an element of type 6^1 and it follows that $V = U$. Assume then that $A \leq B \cdot D_8$. Then

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

there are at least two conjugacy classes of permutations of type 2^2 in B and hence if V fixes a point then $V = U$. So assume that $V \cap B = V_3$. If $A = B \cdot D_8$ then V must contain a permutation of type 2^2 interchanging two blocks of the partition. We may assume that $V = \langle V_3, (35)(46) \rangle$, but then V contains $(12)(35)(46)(34)(78) = (12)(3456)(78)$ which is a contradiction. Thus $A = B \cdot \mathbb{Z}_4$ or $A = B \cdot (\mathbb{Z}_2 \times \mathbb{Z}_2)$ and $U \leq B$, $V = V_3$, and (e)(iii) or (iv) holds.

3. Kronecker classes of field extensions of small degree

Here we investigate further the structure of a Kronecker class $\mathscr{K}$ relative to k containing a field K with $2 \leq |K : k| = n \leq 8$. We assume that K is a minimal field in $\mathscr{K}$. For $n = 2$ it was shown by Saxl in [12] that $\mathscr{K} = \{K\}$ so we shall assume that $3 \leq n \leq 8$. The results of the previous sections give the width and socle number for $\mathscr{K}$, determine all minimal fields in $\mathscr{K}$ and give information about the Galois hull of $\mathscr{K}$. Here we investigate second minimal fields in $\mathscr{K}$. (Recall that a field $L \in \mathscr{K}$ is called second minimal in $\mathscr{K}$ if $k < L' < L$ for some $L' \in \mathscr{K}$ and L is minimal with respect to this property.)

Let L be an arbitrary field in $\mathscr{K}$ and let $\tilde{L}$ be the Galois hull of $L : k$. By the Reduction Theorem in [3, §2], $K \cap \tilde{L} \in \mathscr{K}$ and as K is a minimal field in $\mathscr{K}$, $K = K \cap \tilde{L} \leq \tilde{L}$. Let A be the Galois group of $\tilde{L} : k$ and let U, V be the fixed groups of K, L respectively. Then $U^A = V^A$, $V_A = \bigcap_{a \in G} V^a = \{1\}$ and $|A : U| = n$. (A subgroup V of a group A is said to be *corefree* in A if $V_A = \{1\}$.) Let $H = U_A$, a possibly trivial normal subgroup of A.

First we shall examine the case where $K : k$ is a Galois extension. Here $V \leq U = H$ and $V^A = H$. A subgroup V of a normal subgroup H of a group A, is called an *A-covering subgroup* of H if $V^A = H$. In this case determining all second minimal fields in $\mathscr{K}$ (when such exist) is equivalent to determining all maximal A-covering subgroups V of H such that V is corefree in A. This has been done in [9] for $n = 4$ and in [10] for $n = 8$, so we need to consider the cases $n = 3, 5, 6, 7$. We shall need, now and later, the following generalization of [10, Propositions 2.1 and 2.2].

PROPOSITION 3.1. *Suppose that H is a normal subgroup of index r in a finite group A and that W is an A-covering subgroup of H which is a maximal subgroup of H and is corefree in A. Let S be the socle of H, (the product of the minimal normal subgroups of H). Then either S is elementary abelian or the following hold.*

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

(i) *The socle* $S = N_1 \times \cdots \times N_s$ *is a direct product of* $s \geq 5$ *minimal normal subgroups of* H *where for each* $i \leq s$, $N_i \simeq T^k$ *is a direct product of* $k \geq 1$ *copies of a nonabelian simple group* T. *Moreover if* $s = 5$ *then* $N_i \simeq T = A_5$.

(ii) *The group* A *acts transitively by conjugation on* $\{N_1, \dots, N_s\}$ *and has an orbit* J *on unordered pairs of elements of this set of length* $|J| \geq st/2 \geq 2s$, *where* t *is the number of conjugacy classes of* $\operatorname{Aut} T^k$ *in* T^k. *Moreover if* $|J| = 2s$ *then* $N_i = T = A_5$.

(iii) *For some* $\{N_i, N_j\} \in J$, $W \cap S = D \times (\prod_{l \neq i,j} N_l)$ *where* D *is a diagonal subgroup of* $N_i \times N_j$. *Moreover* r *is divisible by* $|J|$ *and by* s. *In particular* $r \geq 2s \geq 10$.

Proof. Most of the proposition follows from [10, Propositions 2.1 and 2.2 and their proofs], where it is shown that W is as in (iii), $|J|$ divides r and $|J| \geq s$. To obtain the better lower bound on $|J|$ we define a graph Γ with vertex set $V\Gamma = \{N_1, \dots, N_s\}$ and edge set J. Now each element $\mathbf{x}$ of $S = N_1 \times \cdots \times N_s$ lies in $(W \cap S)^a$ for some $a \in A$ and hence the entries in $\mathbf{x}$ in positions i^a and j^a lie in the same conjugacy class of $\operatorname{Aut} T^k$ in T^k. Let $\mathscr{T}$ be the set of such conjugacy classes. Then $\mathbf{x}$ determines a mapping $\phi_{\mathbf{x}} : V\Gamma \to \mathscr{T}$ by defining $(N_i)\phi_{\mathbf{x}}$ to be the conjugacy class containing the ith entry in $\mathbf{x}$, and as $\mathbf{x}$ varies over S all mappings $V\Gamma \to \mathscr{T}$ arise. Thus for each mapping $\phi : V\Gamma \to \mathscr{T}$ there is some edge $\{N_b, N_c\}$ in Γ such that $(N_b)\phi = (N_c)\phi$, that is to say, it is not possible to colour the vertices of Γ with $|\mathscr{T}|$ colours such that adjacent vertices have different colours. Now it is clear that the vertices of a graph of valency v can be coloured by a set of $v + 1$ colours and hence $|\mathscr{T}|$ is at most the valency of Γ, that is $|\mathscr{T}| \leq 2|J|/s$. So $|J| \geq s|\mathscr{T}|/2$ and it was shown in [10, Proposition 2.2] that $|\mathscr{T}| \geq 4$ and $|\mathscr{T}| = 4$ if and only if $N_i = T = A_5$.

Corollary 3.2. *With the notation of Proposition* 3.1, *let* Γ *be the graph with vertex set* $\{N_1, \dots, N_s\}$ *and edge set* $J = \{i, j\}^A$, *where* $W \cap S = D \times (\prod_{l \neq i,j} N_l)$, D *a diagonal subgroup of* $N_i \times N_j$. *Then, if there are* t *conjugacy classes of* $\operatorname{Aut} T^k$ *in* T^k, *the vertices of* Γ *cannot be coloured with* t *colours such that adjacent vertices have different colours.*

Theorem 3.3. *Let* A *be a finite group with a nontrivial normal subgroup* H *of index* n *where* n *is* 3, 5, 6 *or* 7. *Let* V *be a maximal subgroup of* H *which is corefree in* A *and which is an* A*-covering subgroup of* H. *Then up to conjugacy in* A *one of the following holds.*

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

(a) $n = 3$, $A = A_4$, $H = Z_2 \times Z_2$ *and* $V = Z_2$.

(b) n *is* 5 *or* 7, $A \simeq \mathbb{Z}_2^{n-1} \cdot \mathbb{Z}_n$, $H \simeq \mathbb{Z}_2^{n-1}$ *is the subgroup of elements of* $\mathbb{Z}_2^n$ *with an even number of nonzero entries, and* V *is the subgroup of* H *of index 2 consisting of all elements of* H *with first entry zero.*

(c) $n = 6$, A *is* S_4 *or* $A_4 \times \mathbb{Z}_2$, H *is the normal subgroup of* A_4 *of order* 4, *and* V *is a subgroup of* H *of order* 2.

(d) $n = 6$, $A = SR$ *where* $S = \mathbb{Z}_5 \times \mathbb{Z}_5$ *and either* $R = \mathbb{Z}_{24}$ *or* $R = \langle x, y | x^3 = y^8 = 1, y^{-1}xy = x^{-1} \rangle$ *with* R *acting regularly on the six subgroups of* S *of order* 5; $H = S \cdot T$ *where* T *is the normal subgroup of* R *of order* 4, *and* $V = \mathbb{Z}_5 \cdot T$.

(e) $n = 6$, $A = HR$ *where* $H = \mathbb{Z}_2^4$ *and* R *is* S_3 *or* $\mathbb{Z}_6$, *(further* $A_4 \wedge A_4 < A \leq S_4 \operatorname{wr} \mathbb{Z}_2$ *and* R *interchanges the two* S_4*'s);* $V \simeq \mathbb{Z}_2^3$.

(f) $n = 7$, $A = \mathbb{Z}_2^3 \cdot \mathbb{Z}_7$ *is a Frobenius group,* $H = \mathbb{Z}_2^3$ *and* $V = \mathbb{Z}_2^2$.

Remarks. (1) The examples in parts (a) and (b) belong to a general family of examples of covering subgroups: let $N = \mathbb{Z}_2^n$, let H be the subgroup of N of elements with an even number of nonzero entries, and let V be the subgroup of H of elements with first entry 0. Let T be any group of order n, and let $A = H \cdot T$ be the semidirect product with T acting regularly on the n entries of elements in H (so A has index 2 in $NT = \mathbb{Z}_2 \operatorname{wr} T$). Then V is an A-covering subgroup of H if and only if n is odd.

(2) The group theory package CAYLEY [1] was used to verify that the groups given in (d) and (e) are examples and that these are the only groups occurring here up to conjugacy. I am grateful to Derek Holt for some helpful discussions about this. The group A in part (d) is a subgroup of the affine group $\mathrm{AGL}(2, 5)$, and $T \simeq Z_4$ is the subgroup of scalar matrices in $\mathrm{GL}(2, 5)$.

(3) For Kronecker classes $\mathscr{K}$ relative to k containing a Galois extension K of degree 3, 5, 6 or 7, this proposition determines the Galois group A of $\tilde{L} : k$ and the fixed group V of $L : k$ for all second minimal fields $L \in \mathscr{K}$.

Proof. By Proposition 3.1, the socle S of H is elementary abelian. Now A acts transitively and faithfully by right multiplication on the set $\Omega = [A : V]$ of right cosets of V in A and H has $|A : H| = n$ orbits $\Omega_1 = [H : V], \Omega_2, \ldots, \Omega_n$ in Ω on each of which it acts primitively. Since S is abelian, $S(1) = V \cap S$ is the kernel of the action of S on Ω_1 and $S = (V \cap S)^A = \bigcup_{1 \leq i \leq n} S(i)$, where $S(i)$ is the kernel of S on Ω_i. By [9, Lemma 3.1], $S(i) \neq \{1\}$. Now $|S(i)| = |S|/|\Omega_i| = |S|/m$, say, and $S(i)$ is a normal subgroup of H, so $S(i)$ is either trivial or transitive on Ω_j for each j (since H is primitive on Ω_j). Suppose first that $S(i) = S(j)$ for some $i \neq j$. Then $J(i) = \{j | S(j) = S(i)\}$ is a proper nontrivial block of imprimitivity for A in $\{1, \dots, n\}$ (where we let A act on $\{1, \dots, n\}$ in the same way as it acts on $\{\Omega_1, \dots, \Omega_n\}$) and we have

$$|S| = \left|\bigcup S(i)\right| < (n/|J(i)|)|S(i)| = n|S|/m|J(i)|$$

so that $2 \leq m < n/|J(i)| \leq n/2$. Thus $|J(i)| = 2$, $n = 6$, and $m = 2$. If $|S| = 4$ then $H = S > V = Z_2$ and either $A/H = S_3$ and $A = S_4$ as in (c) or $A/H = Z_6$. In the latter case let $A = \langle H, a \rangle$. Then $a^6 \in H$ is centralized by a and as a permutes the 3 involutions in H transitively we have $a^6 = 1$. Also as a^3 normalizes $S(i)$ for all i, a^3 lies in the centre of A. Thus $A = A_4 \times \langle a^3 \rangle$ and (c) is true. If $|S| \neq 4$ then $|S| = 8 = |\bigcup S(i)| = 3.4 - 3.2 + 1 = 7$ by the inclusion-exclusion principle, which is absurd. Thus we may assume that all the subgroups $S(i)$ are distinct. For subsets J of $\{1, \dots, n\}$ we write $S(J)$ for the intersection $\bigcap_{j \in J} S(j)$, and we write $S(\{i, j\})$ as $S(i, j)$ etc.

Next suppose that $S(i, j) = \{1\}$ for some $i \neq j$. Then $|S| = m^2$ and hence $S(i, j) = \{1\}$ for all $i \neq j$. We have $m^2 = |S| = n(m-1) + 1$ so that $n = m + 1$ is 3, 5 or 6. (Note that m is a prime power.) If $n = 3$ then (a) holds. If $n = 5$ then, since H is primitive on each Ω_i and is faithful on $\Omega_1 \cup \Omega_2$ we have $Z_2^4 \cdot Z_3 \leq H \leq S_4 \times S_4$ so that H has only two normal subgroups of order 4 (not the 5 distinct $S(i)$, $1 \leq i \leq 5$). If $n = 6$ then $S = \mathbb{Z}_5 \times \mathbb{Z}_5$ is self-centralizing in A (since any element centralizing S centralizes each $S(i)$ and hence lies in H, and hence in S) and so $A \lesssim \mathrm{AGL}(2, 5)$ and $H = ST$ where $\{1\} \leq T \leq Z(\mathrm{GL}(2, 5)) \simeq Z_4$. We may take $V = S(1) \cdot T$ and A/H is a subgroup of $\mathrm{PGL}(2, 5)$ of order 6 acting regularly on the six subgroups of S of order 5. It follows that (d) holds.

Thus we may suppose that $S(i, j) \neq \{1\}$ for all distinct i, j. If $n = 3$ then $m^3 = |S| = 3m^2 - 3m + 1$, which implies that $m = 1$, which is a contradiction. Thus from now on $n \geq 5$. Suppose now that $S(i, j)$, for $i \neq j$, fixes a third set Ω_k pointwise. Set $J(i, j) = \{k | S(i, j) = S(i, j, k)\}$. Then each pair of points lies in at most one image of $J(i, j)$ under elements of A, each point lies in the same number of images, and the number of images divides n. It follows that $|J(i, j)| = 3$ and either $n = 7$ and we can take the images of $J(i, j)$ as the cyclic shifts of the set $\{1, 2, 4\}$ under the permutation (1234567), or $n = 6$ and there are just two disjoint images, say $\{1, 2, 3\}$ and $\{4, 5, 6\}$ of $J(i, j)$. If $n = 7$ then $S(J) = \{1\}$ for each set J of size 4 so we have

$$\begin{aligned} m^3 = |S| &= 7(m^2 - 3(m-1) - 1) + 7(m-1) + 1 \\ &= 7m^2 - 14m + 8, \end{aligned}$$

that is, $m = 2$ or 4. If $m = 2$ then (f) holds, but if $m = 4$ then, as H is primitive on each Ω_i, H cannot have as many as seven distinct normal subgroups of order 4. If $n = 6$ then applying [9, Lemma 3.2] to $S(1, 2, 3) \times S(4, 5, 6)$ shows that $S(1, 2, 3, 4) \neq \{1\}$ so that $m^4 = |S|$ and $S(1, 2, 3) = S(1, 2, 3, 4)^{A_1}$ where $A_1 = N_A(S(1, 2, 3))$. It follows that $m = 2$, $H = S = Z_2^4$ and $A \leq S_4 \operatorname{wr} S_2$. Now A/H has order 6. Let T be a Sylow 3-subgroup of A. Then T has trivial centralizer in S and so its normalizer $R = N_A(T)$ has order 6 and is a complement for H in A, R must interchange $S(1, 2, 3)$ and $S(4, 5, 6)$ and there are examples with $R \simeq S_3$ and $R \simeq Z_6$. Thus (e) holds.

We may now assume that $S(i, j)$ fixes only $\Omega_i \cup \Omega_j$ pointwise. If $|S| = m^3$ then

$$m^3 = n(m^2 - (n-1)(m-1) - 1) + n(n-1)(m-1)/2 + 1;$$

this equation has no prime power solutions m for $n = 5, 6, 7$. Thus $|S| \geq m^4$ and $S(J) \neq \{1\}$ for subsets J of size 3. Suppose that $S(i, j, k)$ fixes a fourth Ω_l pointwise and set $J(i, j, k) = \{l | S(i, j, k) = S(i, j, k, l)\}$. Then each 3-subset lies in at most one image of $J(i, j, k)$, each point lies in the same number of images and the number of images divides n. Thus $|J(i, j, k)| = 4$ and either $n = 7$ and we may take the $J(i, j, k)$ to be the images of $\{1, 2, 3, 5\}$ under (1234567), or $n = 6$ and we may take the images as $\{1, 2, 3, 4\}$, $\{1, 2, 5, 6\}$, and $\{3, 4, 5, 6\}$. If $n = 7$ then $S(J) = \{1\}$ for any 5-set J so

$$m^4 = |S| = 7m^3 - 21m^2 + 35m - (7m+28) + 21 - 7 + 1 = 7m^3 - 21m^2 + 28m - 13$$

which has no solutions. If $n = 6$ then by [9, Lemma 3.2] for each 5-set J, $S(J) = \{1\}$, and so

$$m^4 = |S| = 6m^3 - 15m^2 + 20m - (3m + 12) + 6 - 1 = 6m^3 - 15m^2 + 17m - 7$$

which has no solutions. Thus $S(i, j, k)$ fixes only $\Omega_i \cup \Omega_j \cup \Omega_k$ pointwise for all distinct i, j, k. If $|S| = m^4$ then

$$m^4 = nm^3 - \binom{n}{2} m^2 + \binom{n}{3} m - \binom{n}{4} + \binom{n}{5} + \cdots + (-1)^{n-1},$$

and hence $n = 5$, $m = 2$ and (b) holds. So we may assume that $|S| \geq m^5$. By [9, Lemma 3.2], $n \geq 6$, and $|S| \leq m^{n-1}$. Then if $n = 6$ we have

$$m^5 = |S| = 6m^4 - 15m^3 + 20m^2 - 15m + 6 - 1$$

which has no solutions. Thus $n = 7$. If, for some J of size 4, $S(J)$ fixes a fifth Ω_k pointwise then $S(J) = S(J \cup \{k\})$ fixes exactly 5 of the Ω_i and

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

the stabilizer of every 4-set fixes 5 of the Ω_i; we then have

$$m^5 = |S| = 7m^4 - 21m^3 + 35m^2 - 35m + (7m + 14) - 7 + 1$$

which has no solutions. Thus $S(J)$ fixes only 4 of the Ω_i and we have

$$|S| = m^{5+\delta} = m^\delta(7m^4 - 21m^3 + 35m^2 - 35m + 21) - 7 + 1$$

where δ is 0 or 1. It follows that $|S| = 2^6$ and (b) holds. This completes the proof of Theorem 3.3.

Now we consider the case where the extension $K : k$ is not Galois. Here $U \neq H$. Theorem 2 lists all the possibilities for the groups A/H, U/H and VH/H. Thus if U is corefree in A, that is, if $H = \{1\}$, then all possibilities for the groups A, U and V are given by Theorem 2 (a), (b), (d), (e), and all of these groups V correspond to minimal fields L in $\mathscr{K}$. (Note that the groups in part (c) do not give examples here since K minimal implies that U is not a proper subgroup of V.) Thus if L is second minimal in $\mathscr{K}$ then $H = U_A$ is nontrivial, and, as V is corefree in A, $V \neq VH$. Further $U^A = V^A = (VH)^A$, so if VH is the fixed group of the subfield L' of $\tilde{L}$ then L' is a minimal field in $\mathscr{K}$ and L' is contained in L. Now if M is a maximal subgroup of VH containing V then $M^A = V^A$ so, for L'' the subfield of $\tilde{L}$ with fixed group M, we have $L'' \in \mathscr{K}$ and $L' < L'' \leq L$. Thus if L is second minimal in $\mathscr{K}$ then V is a maximal subgroup of VH. Determining all second minimal fields in $\mathscr{K}$ in this case is equivalent to determining all maximal subgroups V of VH which are corefree in A and satisfy $V^A = (VH)^A$, where A/H, U/H, and VH/H satisfy one of the conclusions (a) to (e) of Theorem 2. We are able to complete this classification for $n = 3$ and $n = 4$ and we discuss further the cases of larger $n \leq 8$.

From now on let A, U, VH, V be as in the previous paragraph with V maximal in VH, and let $t = |A : VH|$. Clearly $V \cap H$ is an A-covering subgroup of H and if W is a maximal subgroup of H containing $V \cap H$ then W is also an A-covering subgroup of H. Moreover, as we see below, W is corefree in A (see Figure 1).

LEMMA 3.4. *Suppose that a finite group A has a normal subgroup H and a corefree subgroup V such that V is a proper maximal subgroup of VH. If W is a maximal subgroup of H which contains $V \cap H$ then W is also corefree in A.*

PROOF. Since V is corefree, A acts faithfully and transitively by right multiplication on the set $\Omega = [A : V]$ of right cosets of V in A. As V is

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

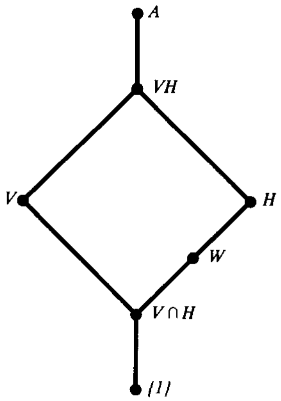

FIGURE 1

maximal in VH, the set $\Delta = [VH : V]$ of cosets of V in VH is a minimal block of imprimitivity for A in this action. The subgroup V is the stabilizer of the point $\delta = V \in \Delta$ and $V \cap H$ is the subgroup of H fixing δ. Thus W is intransitive on Δ and hence W_A is intransitive on Δ. Since W_A is a normal subgroup of VH and VH acts primitively on Δ it follows that W_A fixes Δ pointwise and hence that $W_A = \{1\}$.

Let S be the socle of H (the product of the minimal normal subgroups of H). Now, as V is corefree in A, A acts faithfully and transitively on the set $\Delta = [A : V]$ of right cosets of V in A, and the set $\Sigma_1 = [VH : V]$ is a block of imprimitivity. Since V is maximal in VH, the setwise stabilizer VH of Σ_1 acts primitively on Σ_1, and its normal subgroup S acts transitively on Σ_1. Let $\Sigma = \{\Sigma_1, \dots, \Sigma_t\}$ be the set of images of Σ_1 under elements of A and, for $1 \leq i \leq t$, let $S(i)$ denote the kernel of S on Σ_i. Then $S(1) = (V \cap S)_H$. We shall consider A permuting the index set $\{1, 2, \dots, t\}$ in the same way that it permutes Σ; for $J \subseteq \{1, 2, \dots, t\}$ we shall write $S(J)$ for the intersection $\bigcap_{j \in J} S(j)$, and we shall write $S(i, j)$ for $S(\{i, j\})$ etc.

First we consider the case where S is nonabelian.

LEMMA 3.5. *If n is 3 or 4 then S is elementary abelian. If S is nonabelian (and hence $n \geq 5$) then VH induces on Σ_1 a primitive group of (simple or compound) diagonal type.*

Recall that a primitive group is said to be of *diagonal type* if its socle $S = T^{kl}$, for a nonabelian simple group T and $k \geq 1$, $l \geq 2$, and the stabilizer of a point in S is a direct product D^k where $D \simeq T$ is a diagonal subgroup of a product T^l of l of the simple direct factors of S (see [8]).

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

PROOF. Suppose that S is not elementary abelian. By Lemma 3.4, W is corefree in A. By Proposition 3.1, $S = N_1 \times \cdots \times N_s$ where $s \geq 5$ and each $N_i \simeq T^k$ for some nonabelian simple group T and $k \geq 1$. The N_i are minimal normal subgroups of H and are conjugate in A. Also we may take $W \cap S$ to be $D \times N_3 \times \cdots \times N_s$, where D is a diagonal subgroup of $N_1 \times N_2$. Now $V \cap S \leq W \cap S$ so $S = N_I \times S(1)$ for some $I \subseteq \{1, 2, \ldots, s\}$, where $N_I = \prod_{i \in I} N_i$ acts faithfully on Σ_1 and $\{1, 2\} \subseteq I$. Since $(V \cap S)^A = S$, by [9, Theorem 2.1] we have $V \cap S \simeq T^{k'}$ and $V \cap S$ is a subdirect product of $\prod N_i$. Thus by the O'Nan Scott Theorem [8], VH^{Σ_1} is a group of diagonal type. Now VH^{Σ_1} has at most two minimal normal subgroups so either VH is transitive on I or has two orbits I_1 and I_2 of equal length in I. Define a graph $\tilde{I}$ with vertex set I and edges the images under VH of the pair $\{1, 2\}$ (considering A to act on the index set $\{1, 2, \ldots, s\}$ as it acts on $\{N_1, \ldots, N_s\}$). Then as V is maximal in VH it follows that $V \cap S$ is a product of a diagonal subgroup D_C of $\prod_{j \in C} N_j$ for each connected component C of $\tilde{I}$ and VH is transitive on these components. (Moreover if VH has two orbits I_1 and I_2 in I then I_1 contains points of each component. If $I = \{1, 2\}$ then $V \cap S = W \cap S$ so $V \cap H = W$ and the orbit $\{1, 2\}^A$ has length dividing $|A : VH| = t$; by Proposition 3.1 we have $t \geq 2s \geq 10$ so that by Theorem 2, $n = 5$, $t = 10$ and $s = 5$, $N_i = A_5$. Thus we may assume that $|I| \geq 3$.)

As in the proof of Proposition 3.1, each $\mathbf{x} \in S$ determines a mapping $\phi_{\mathbf{x}} : \{1, \ldots, s\} \to \mathcal{T}$ where $\mathcal{T}$ is the set of $\operatorname{Aut} T^k$ classes in T^k and $i\phi_{\mathbf{x}}$ is the class containing $\mathbf{x}_i$. Elements of $\mathcal{T}$ may be considered as "colours" and $\phi_{\mathbf{x}}$ as a colouring of the set $\{1, \ldots, s\}$. For $\mathbf{x} \in V \cap D$, $\phi_{\mathbf{x}}$ is constant on each connected component of $\tilde{I}$, that is, each connected component of $\tilde{I}$ is monochromatic with respect to this colouring. Then since $(V \cap S)^A = S$, each $\mathbf{x}$ in S lies in $(V \cap S)^a$ for some $a \in A$ and hence with respect to the colouring induced by $\phi_{\mathbf{x}}$, the connected components of the graph $\tilde{I}^a$ are all monochromatic. Thus for each colouring of $\{1, \ldots, s\}$ by the colour set $\mathcal{T}$ there is some $a \in A$ such that the components of the graph $\tilde{I}^a$ are monochromatic.

Suppose that $n = 3$. Then by Theorem 2, also $t = 3$, $A/H = S_3$, and as $s \geq 5$ divides $|A/H|$, $s = 6$. Since there are three distinct images of I under elements of A, with each of $1, \ldots, y$ belonging to a constant number of them it follows that $|I| = 4$. Now S contains an element $\mathbf{x}$ with $x_1 = x_2 = x_3 = 1$, and the other three entries in distinct nontrivial $\operatorname{Aut} T^k$-conjugacy classes in T^k. The corresponding colouring $\phi_{\mathbf{x}}$ does not have the required property for any set I of size 4. Thus $n \geq 4$.

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

Suppose that $n = 4$ so by Theorem 2, $t = 4$. Now $|VH^I|$ divides $|VH/H|$ which divides 6. If 3 divides $|VH^I|$ then $|I|$ is 3, 6 or 12. If not then $|VH^I|$ divides 2 so $|I| = 4$ and VH^I has two orbits of length 2. If $|I| = 12$ then VH^I has two orbits of length 6 so $A/H = S_4$ and, as $s > |I|$, $s = 24$; here I_1 say is a block of length 6 and colouring the four images of I_1 monochromatically with four different colours gives a contradiction. Thus $|I| \neq 12$. If $s = 24$ then $A/H = S_4$, and $|I| = 6$ and I is a block of imprimitively for A; if we colour each image of I using four colours then no component of any image of $\tilde{I}$ is monochromatic. Thus $s < 24$. Suppose next that $s = 12$. Then 3 divides $|VH^I|$ so $|I|$ is 3 or 6. In the former case I is a block of imprimitivity and colouring the three points of each block with three different colours gives a contradiction. Thus $|I| = 6$. If VH^I has two orbits of length 3 then I_1 is a block and colouring each image of I_1 monochromatically with a different colour gives a contradiction. Thus VH^I is transitive, $A/H = S_4$, and either VH has two orbits of length 6 in $\{1, \dots, 12\}$ or VH is the stabilizer of a block B in $\{1, \dots, 12\}$ of size 3. In the former case I consists of one point from each of six blocks of length 2, and colouring these blocks monochromatically using four colours yields a contradiction. In the latter case, I consists of two points of three of the images of B and colouring the images of B monochromatically with four different colours or colouring two monochromatically and two using three colours yields a contradiction. Thus $s < 12$. If $s = 8$ then VH is the stabilizer of a block B in $\{1, \dots, s\}$ of size 2 and is transitive on the other six points. Thus $|I| = 6$ and VH transitive on I. Then colouring the images of B monochromatically with four different colours yields a contradiction. Thus as $s \geq 5$ and s divides 24, $s = 6$, A/H is A_4 or S_4, and as 3 divides $|VH^I|$ and $s > |I|$ we must have $|I| = 3$. It is possible to colour $\{1, \dots, 6\}$ with 4 colours with no monochromatic triple. Thus $n \neq 4$.

Remarks. The cases $5 \leq n \leq 8$ are much more tedious but the techniques above would probably be sufficient to determine whether H could have a nonabelian socle. In particular, if the subset I above had size 2 we saw that $n = 5$, $t = 10$, $s = 5$, and $A/H = A_5$ (by Theorem 2) and $N_i \simeq A_5$ (by Proposition 3.1); also $VH^{\Sigma_1} \leq (A_5 \times A_5) \cdot (\operatorname{Out} A_5 \times S_2)$ and it follows that $S = A_5^5$ and $H = S$ or $S \cdot 2$. For $V \cap S$ to be an A-covering subgroup of S it is necessary for $V \cap S$ to contain elements of the form $(x, x, 1, 1, 1)$ and $(x, x', 1, 1, 1)$ where x, x' are of order 5 but not conjugate in A_5. With $A \leq (A_5 \cdot 2) \cdot A_5$ this was seen to be not possible (using CAYLEY to check some calculations). Thus always the set I has size at least 3.

Now we assume that S is elementary abelian. Then S is regular on each Σ_i and so $V \cap S = S(1)$ and $S = \bigcup_{1 \leq i \leq t} S(i)$; also $|\Sigma_i| = m$ is a prime power and $|S(i)| = |S|/m$. By [9, Lemma 3.1 and 3.2], $S(i) \neq \{1\}$, $S(i)$ is trivial or transitive on each Σ_j, and $S(J) = \{1\}$ for each subset J of $\{1, \dots, t\}$ of size $t-1$, so $m^2 \leq |S| = m^a \leq m^{t-1}$.

Lemma 3.6. *If $3 \leq n \leq 8$ then $|S| \leq m^{t-2}$. In particular, $n \geq 4$ and $t \geq 4$.*

Proof. Suppose that $|S| = m^{t-1}$. Then by the inclusion-exclusion principle we have

$$m^{t-1} = \left|\bigcup S(i)\right| = \sum_{1 \leq i \leq t-1} (-1)^{i-1} \binom{t}{i} m^{t-1-i} + (-1)^{t-1},$$

that is $(m-1)^t = (-1)^{t-1}(m-1)$ and hence $m = 2$ and t is odd. If $n = t$ then, in its action on Δ, A is a subgroup of index 2 in $S_2 \operatorname{wr} T \leq S_{2t}$ where $T \simeq A/H$ is a transitive nonregular subgroup of S_t; the subgroup $H = S$ is the subgroup of the base group S_2^t of all t-tuples with an even number of nonzero entries and $V \cap H$ is the subgroup of H of t-tuples with first entry zero. For $n = t = 3, 5, 7$ and for all possible subgroups T we can check that the extension A of H by T splits, that is, $A \simeq H \cdot T$; in all cases we find an element of VH which has no fixed point in Δ so that $V^A \neq (VH)^A$, a contradiction. (For example, take the blocks of size 2 to be $\{2i-1, 2i\}$, $1 \leq i \leq t$. Then VH contains $x = (12)(34)$, and, if $|T|$ is even and T is not $\mathrm{PSL}(2, 7)$ of degree 7, then V contains an element y such that yH has order 2 and y fixes only the block $\{1, 2\}$ setwise; then $xy \in VH$ and xy is fixed point free. If $T = \mathrm{PSL}(2, 7)$ or $|T|$ is odd (in which case T is a Frobenius group of order 21) we take $y \in V$ with yH of order 3.)

On the other hand if $n \neq t$ and t is odd then by Theorem 2, $n = 6$, $t = 3$, $A/H = A_4$ and VH is a normal subgroup of A of index 3. However in its action on Δ of degree $tm = 6$ we have $A \leq S_2 \operatorname{wr} S_3$ so that a Sylow 3-subgroup of A cannot normalize a subgroup of order 16. Thus $m^2 \leq |S| \leq m^{t-2}$ so $t \geq 4$, and by Theorem 2, $n \geq 4$.

Lemma 3.7. *If $4 \leq n \leq 8$ and $|S| = m^2 \leq m^{t-2}$ then $t = m+1 \in \{4, 5, 6, 8, 10\}$ or $t = 8$, $m = 3$. Moreover if $n = 4$ then $t = 4$, $A = SQ <$ $\mathrm{AGL}(2, 3)$, where $Q = \langle \left(\begin{smallmatrix} 2 & 2 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ is a Sylow 2-subgroup of $\mathrm{GL}(2, 3)$, $H = SZ(Q)$, $S = \mathbb{Z}_3^2$, and $V = S(1) \cdot \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), -I \rangle$.*

Proof. Suppose that $|S| = m^2$. Then each $S(i)$ has order m, and distinct $S(i)$ intersect in $\{1\}$. Since $S = \cup S(i)$ we have $m^2 = r(m-1) + 1$

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press

where r is the number of distinct subgroups $S(i)$. Hence (see Theorem 2) either $t = r = m + 1 \in \{4, 5, 6, 8, 10\}$ or $t = 2r = 2(m+1) \in \{6, 8, 10\}$.

Suppose that $t = 2r = 6$, $m = 2$. Then $A \leq S_2 \operatorname{wr} S_6$ and, as $|H| = 4$, A has 3 blocks of imprimitivity of size 4 and each nontrivial element of H fixes exactly four points, namely one of the blocks. By Theorem 2, $n = 6$ and as $U \neq H$ also $VH \neq H$. It follows that V contains a 2-element y which fixes only two of the blocks of size 2 setwise. Then for $x \in H - S(1)$, $xy \in VH$ is fixed point free so that $V^A \neq (VH)^A$. Suppose that $t = 2r = 10$, $m = 4$. Then by Theorem 2, $n = 5$, $A/H = A_5$ and $VH/H = S_3$. Now VH fixes only one of the Σ_i setwise, namely Σ_1. On the other hand, as $S(1) = S(i)$ for some $i > 1$ (since there are only five distinct $S(i)$), the stabilizer of Σ_1 also fixes Σ_i, which is a contradiction.

Suppose now that $n = 4$. Then, $t = 4$, $m = 3$, and the four subgroups $S(i)$ are all distinct. It follows that S is self-centralizing in A and hence that $A/S \lesssim \mathrm{GL}(2, 3)$. Now $A \lesssim S_{12}$ and A has a set Σ of 4 blocks of size 3. If V contains an element y fixing only one block setwise and fixing that block pointwise then for some $x \in H$, $xy \in VH$ is fixed point free and so $(VH)^A \neq V^A$. If $A/H \geq A_4$ then a 3-element y in $V \backslash S(1)$ has this property so we must have $A/H = D_8$ and hence $A = S \cdot Q$ where Q is a Sylow 2-subgroup of $\mathrm{GL}(2, 3)$, and $H = X \cdot Z(Q)$. Taking $Q = \langle \left(\begin{smallmatrix} 2 & 2 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ we may assume that $VH = S \cdot V \cap Q$ where $V \cap Q = \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), -I \rangle$ and it is readily checked that VH contains no fixed point free elements, that is, $(VH)^A = V^A$.

References

[1] J. J. Cannon, 'An introduction to the group theory language Cayley', *Computational group theory*, edited by M. Atkinson, pp. 145–183, (Academic Press, New York, 1984).

[2] R. M. Guralnick, 'Zeroes of permutation characters with applications to prime splitting and Brauer groups,' (1988) preprint.

[3] W. Jehne, 'Kronecker classes of algebraic number fields', *J. Number Theory* **9** (1977), 279–320.

[4] W. Jehne, 'Kronecker classes of atomic extensions', *Proc. London Math. Soc.* (3) **34** (1977), 32–64.

[5] N. Klingen, 'Zahlkörper mit gleicher Primzerlegung', *J. Reine Angew. Math.* **229/300** (1978), 342–384.

[6] N. Klingen, 'Atomare Kronecker-Klassen mit speziellen Galoisgruppen', *Abh. Math. Sem. Univ. Hamburg.* **48** (1979), 42–53.

[7] N. Klingen, 'Rigidity of decomposition laws and number fields', *J. Austral. Math. Soc., Ser. A*, (to appear).

[8] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan-Scott Theorem for finite primitive permutation groups', *J. Austral. Math. Soc., Ser. A* **44** (1988), 389–396.

[9] C. E. Praeger, 'Covering subgroups of groups and Kronecker classes of fields', *J. Algebra.* **118** (1988), 455–463.

[10] C. E. Praeger, 'On octic extensions and a problem in group theory', *Group theory*, Proceedings of the 1987 Singapore Conference, edited by K. N. Cheng and Y. K. Leong, pp. 443–463, De Gruyter, (Berlin, New York, 1989).

[11] C. E. Praeger, 'On the inclusion problem for primitive permutation groups', *Proc. London Math. Soc.* (3), **60** (1990), 68–88.

[12] J. Saxl, 'On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields', *Proc. London Math. Soc.* (to appear).

[13] C. C. Sims, 'Computational methods in the study of permutation groups', *Computational problems in abstract algebra*, edited by J. Leech, pp. 169–183, (Pergamon Press, Oxford, London, 1970).

Department of Mathematics
University of Western Australia
Nedlands WA 6009
Australia

https://doi.org/10.1017/S1446788700032766 Published online by Cambridge University Press